

PLAINTIFF'S
EXHIBIT

2

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF TEXAS
BEAUMONT DIVISION

Bruce Cohn,

Plaintiff,

v.

Anna Popescu, TrustHFTwallet.com,
and John Does 1 – 20,

Defendants.

Case No. 1:24-cv-00337

Declaration of Evan Cole

I, Evan Cole, state and swear as follows.

I. Introduction

1. My name is Evan Cole. I am of sound mind and capable of making this Declaration. I have personal knowledge of the facts stated herein.

2. I am the founder of Digital Investigations, LLC. I am experienced in blockchain investigations and am knowledgeable about the pig-butcherering scam epidemic and the tactics of cybercriminals like the Defendants in this case. I hold the Chainalysis Cryptocurrency Fundamentals and the Chainalysis Reactor Certifications.

3. Bruce Cohn has retained my firm to provide blockchain analysis and expert-witness services. I am submitting this Declaration in support of Mr. Cohn's Motion for Preliminary Injunction (the "Motion").

II. Pig-Butchering Scams

4. Attachment A to this Declaration is a true and correct preprint of a forthcoming academic article titled *Deconstructing a Form of Hybrid Investment Fraud: Examining 'Pig Butchering' in the United States* (hereafter “*Examining Pig Butchering*”), which will be published in the Journal of Economic Criminology in September 2024.¹

5. *Examining Pig Butchering* aims to situate pig-butchering scams within the broader typology of cyber-enabled fraud. It does so by reviewing the “tactics, tools, and methods of operation” on display in a database of more than 1,300 news articles and court documents compiled by the authors. The result is what I believe to be the most comprehensive academic study of the pig-butchering epidemic to date.

6. Pig-butchering scams have distinctive characteristics. Any experienced investigator can spot one immediately. Nevertheless, the typology set out in *Examining Pig Butchering* is crucial. By compiling and analyzing an enormous trove of reported cases, the authors have provided a framework for objectively determining whether a pig-butchering scam is at issue in a given case.

7. To make such a determination here, I first Mr. Cohn’s declaration submitted in support of the Motion. I then compared the evidence

¹ Marie-Helen Maras, Emily R. Ives, *Deconstructing a Form of Hybrid Investment Fraud: Examining 'Pig Butchering' in the United States*, JOURNAL OF ECONOMIC CRIMINOLOGY, Volume 5 (forthcoming Sep. 2024).

provided by Mr. Cohn to the paradigm that emerges from *Examining Pig Butchering*. The results are as follows.

8. *Initial Contact.* Mr. Cohn's initial contact with the TrustHFTwallet scam was through a dating website, where she presented herself as a well-heeled and successful businesswoman and investor.² *Examining Pig Butchering* confirms that pig-butcherer victims' first contact with perpetrators is often through social-media platforms, and that perpetrators frequently "display wealth" that is "purportedly made possible by their investments in securities or commodities."³

9. *Cultivating the Relationship.* After contacting Mr. Cohn on the dating website, Popescu asked they continue their conversation on WhatsApp.⁴ There, she told Mr. Cohn that she had been trading and investing in crypto for six years, and offered to "teach [him] how to make money in the short-term Bitcoin market."⁵

10. Comparing these facts with *Examining Pig Butchering*, we see again that Mr. Cohn's experience matches the paradigm precisely. Pig-butcherers consistently begin their relationship with victims by leaving behind the social-media platform or dating app where initial contact was

² Declaration of Bruce Cohn (henceforth, "Cohn Decl."), at ¶¶ 3 – 4.

³ *Examining Pig Butchering* (henceforth, "EPB"), at p.9 (describing initial contact methods), p. 10 (describing displays of wealth).

⁴ Cohn Decl., Att. A, *passim*.

⁵ Cohn Decl. Att. A, at COHN0025.

made, moving their discussions to secure messaging apps like WhatsApp, Skype, or Telegram.⁶ And they frequently offer to act as teachers, promising to impart their insider crypto-trading knowledge to their victims, going to great lengths to establish their purported expertise and qualifications.⁷

11. *Securing the Investment.*' Popescu presented herself as an expert in making profits using a particular crypto-trading platform: TrustHFTwallet.⁸ She walked Mr. Cohn through the process of creating or funding his own accounts at legitimate cryptocurrency exchanges, purchasing cryptocurrency with U.S. dollars using those exchange accounts, making a TrustHFTwallet account, and then transferring those assets to deposit addresses provided by TrustHFTwallet.⁹

⁶ EPB, at p.9 ("Following initial contact, most cases in our dataset revealed that offenders encouraged communications to continue off social media [platforms] ... to other messaging platforms (e.g., WhatsApp, WeChat, Line, Skype, and Telegram.").

⁷ EPB, at p.10 ("In this stage, the offender turns conversations towards investments. The offender then discusses expertise and/or prior success with investments. The goal of these conversations is to introduce the target to a lucrative investment opportunity, and then entice them to invest (which is the next stage."), p.11 (noting that, in the studied cases, "[a] comfort level was established investing to encourage victims to invest more over time ... by offenders offering to teach victims how to trade.").

⁸ Cohn Decl., Att. A, at COHN0022 (Popescu introducing Mr. Cohn to TrustHFTwallet for the first time).

⁹ See, e.g., Cohn Decl., Att. A, at COHN0025-75 (Popescu walking Mr. Cohn through each step of creating and funding TrustHFTwallet account).

12. When Mr. Cohn transferred assets to TrustHFTwallet, his “account balance” on the platform would grow accordingly.¹⁰ He could then watch in real time as his profits grew.¹¹ This growth inspired confidence, which Popescu exploited to induce him to make ever-larger deposits. His ‘balance’ eventually reached \$5,191,779.30.¹²

13. Again, this trajectory is as expected. Pig-butcherers commonly present themselves as having insider knowledge about how to make profits using a particular platform, to which they direct their victims.¹³ They then walk victims through the process of transferring assets to deposit addresses controlled by that platform, continuing to act as a ‘teacher’ along the way.¹⁴ And once the assets are ‘deposited,’ the fake trading platform appears—from

¹⁰ Cohn Decl., Att. D, at COHN0345-0365 (showing transactions with TrustHFTwallet).

¹¹ Cohn Decl., Att. D, at COHN0379 (showing balance of more than \$5,000,000.00)

¹² *Id.*

¹³ EPB, p.11 (noting that typical “confidence building” tactics include “feigning insider knowledge of and connections to investment platforms”).

¹⁴ EPB, p. 10 (“[O]ffenders encouraged victims to purchase cryptocurrencies, such as Binance Coin (BNB), Bitcoin (BTC), USD Coin (USDC), Tether (USDT), and Ethereum, and deposit them into accounts, apps, and/or online platforms, controlled by the offender(s) and/or associates.”), p. 12 (noting that in most cases “victims were directed to legitimate cryptocurrency exchanges … to create a cryptocurrency account, and then directed to investment apps and platforms controlled by the offenders”).

the victim's perspective—to work as intended.¹⁵ The 'deposits' are reflected, the 'trades' are executed, and the 'profits' rapidly increase.¹⁶

14. *Blocking the Exits.* Mr. Cohn was able to withdraw nearly \$100,000.00 of crypto assets from the TrustHFTwallet platform.¹⁷ But, in mid-July, he tried to make larger withdrawals of approximately \$50,000.00 worth of crypto assets at a time.¹⁸ He was repeatedly blocked from doing so. TrustHFTwallet 'support' told Mr. Cohn that his account had withdrawal restrictions, such that he could only withdraw more assets if he "upgraded" to the "VIP2 Level."¹⁹ He was told that this would require my account to have a value of \$10 million.²⁰

15. Through to the scams' denouement, Mr. Cohn's experience continued to match the pig-butchering pattern. The fact that Mr. Cohn was able to make nearly \$100,000.00 worth of withdrawals confirms that he experienced one of the pig-butchering scammers' most sophisticated strategies: allowing *some* withdrawals, near the beginning of the scam, to cement the victim's trust in the platform. *Examining Pig Butchering* discusses this tactic in detail, noting that allowing these early withdrawals

¹⁵ EPB, p. 11 (noting that "perpetrators often falsely depict invested funds increasing on fake online platforms and apps").

¹⁶ *Ibid.*

¹⁷ Cohn Decl., ¶ 7.

¹⁸ Cohn Decl., ¶ 8.

¹⁹ Cohn Decl, Att. E, COHN0395-0397.

²⁰ *Id.*

“alleviate[s] [victims’] concerns and serve[s] as proof of the app and/or platform’s legitimacy.”²¹

16. Eventually, however, the scammers’ willingness to allow early withdrawals runs out. After this point, pig-butcherering scams’ most consistent feature is how they end: with purported customer-service issues and endless requests for enormous fees.²² Just as in Mr. Cohn’s case, victims are often told that “security issues” have caused their accounts to be flagged—but that they can smooth the process by increasing their account balance even further.²³ Victims’ frantic research, at this stage, usually leads them to discover that they have been the victim of this new type of cyber-scam.²⁴

17. *Conclusion.* The characteristics of pig-butcherering scams are sufficiently distinctive that experienced investigators can recognize them immediately, as I did in this case. There is no doubt that TrustHFTwallet is

²¹ EPB, p.11 (“In several cases in our dataset, victims could withdraw some of their deposited funds from their investments, at least initially. In another case, one victim mentioned that in order to test his control over funds he invested (and to check the legitimacy of the platform), he withdrew money and then deposited it again in his ‘investment’ account. To this victim and others in our dataset, the success of this test (or tests, as certain victims were able to make more than one withdrawal) alleviated concerns and served as proof of the app and/or platform’s legitimacy.”).

²² EPB, p.14 (noting that victims realized they were the victims of scams after being asked to pay “risk deposit fees,” requests that they pay “taxes,” or other “excuses … as to why payment of funds could not be made”).

²³ EPB, p.11 (describing perpetrators’ practice of creating “fake supporting documentation” to “establish legitimacy of false narratives”).

²⁴ EPD, p.13 (describing common situation in which, after receiving demands for payment of various fees and taxes, victims “conduct research” and realize they have been the victim of a pig-butcherering scam).

a fraudulent platform and that Mr. Cohn was the victim of a pig-butchering scam perpetrated by the Defendants.

A. Pig-Butchering Perpetrators

18. *Examining Pig Butchering* also helpfully collects information about the identities, locations, and organizational structures of pig-butchering perpetrators.²⁵ These perpetrators are known to “force[] trafficked victims to conduct” pig-butchering scams in “Cambodia, Laos, Thailand, and Malaysia,” where the pig-butchering business model originated.²⁶

19. The authors’ dataset further “revealed organized criminal groups operating in concert to commit” pig-butchering scams.²⁷ These groups are divided into various units, each responsible for a distinct aspect of the operation of the scams. Specifically, these units took on roles as (i) solicitors, (ii) trading firms, and (iii) shell companies.²⁸ The “solicitors” contact victims, form relationships, and ultimately act as guides to investing in the fraudulent platform.²⁹ The “trading firms” take on the significant technological challenge of ensuring that the fake platform operates with

²⁵ Much of the information recounted here has been previously revealed by law-enforcement agencies and investigative journalists, as reflected in the attachments to my prior Declaration.

²⁶ *EPB*, p.8 (describing geographic dispersion of pig-butchering organizations).

²⁷ *EPB*, p.8 (setting out examples showing “syndicate” structures).

²⁸ *Ibid.*

²⁹ *Ibid.*

sufficient verisimilitude to deceive victims.³⁰ And the “shell companies” take on the task of opening and maintaining the web of deposit addresses and financial accounts used to receive, launder, and hide victims’ assets.³¹

20. Finally, *Examining Pig Butchering* also finds that pig-butchering perpetrators utilize standard methods for laundering and obfuscating stolen assets. The proceeds of pig-butchering scams are typically “commingled and deposited into numerous accounts,” or “rapidly transferred into and out of multiple intermediary wallet addresses,” or “convert[ed] from one form of cryptocurrency to another.”³² These practices are designed to “make it harder to trace stolen cryptocurrency,” making it “more difficult to identify, investigate, and prosecute them.”³³

B. The Scale & Impact of Pig-Butchering Scams

21. Attachment B to this Declaration is a true and correct copy of a CNN article titled *Killed By a Scam: A Father Took His Life After Losing His Savings to International Gangs – [and] He’s Not the Only One*, published on June 17, 2024.

22. This article first describes the tragic story of a father who took his own life after realizing that he had lost his life savings to a pig-butchering

³⁰ *Ibid.*

³¹ *Ibid.*

³² EPB, p.13 (describing laundering and obfuscation tactics).

³³ *Ibid.*

scam.³⁴ It then discusses the shocking scale of the pig-butchering epidemic, noting that “[i]t’s theft at a scale so large that investigators are now calling it a mass transfer of wealth from middle-class Americans to criminal gangs.”³⁵ The article quotes an FBI estimate that in 2023 alone, pig-butchering scams stole nearly \$4 billion from tens of thousands of American victims.³⁶ Finally, the writer quotes Erin West—a California prosecutor leading numerous criminal cases against pig-butchering scammers—who captures the uniquely tortuous nature of pig-butchering cases. To wit:

I’ve been a prosecutor for over 25 years, [and] I’ve done all kinds of different types of crime. I spent nine years in sexual assault. And I’ve never seen the absolute decimation of people that I’ve seen as a result of pig butchering.³⁷

23. Everything in *Killed by a Scam* is consistent with my professional experience investigating pig-butchering cases.

III. Cryptocurrency Transactions

24. It is very easy to move cryptocurrencies on the blockchain. Crypto assets can be moved in seconds from address to address or exchange to exchange. And, as confirmed in *Explaining Pig Butchering*, this is precisely what the pig-butcherers do to cover their tracks and place the assets they have stolen beyond reach.³⁸ Based on my experience, if the Target Accounts

³⁴ Att. B, pp. 1-2.

³⁵ Att. B, p. 3.

³⁶ Att. B, p.3.

³⁷ Att. B, p.3.

³⁸ Att. A, p.13 (describing typical crypto-laundering tactics).

do not continue to be frozen, it is likely that those assets will be further dissipated, which would prevent Mr. Cohn from recovering the assets stolen from him, thereby causing significant and irreparable harm.

[SIGNATURE PAGE FOLLOWS]

VERIFICATION

I, Evan Cole, hereby verify and declare under penalty of perjury
that the foregoing is true and correct.

A handwritten signature consisting of stylized initials "EC" followed by a surname.

Evan Cole

Dated: 9/6/24



2-A

Contents lists available at ScienceDirect

Journal of Economic Criminology

journal homepage: www.journals.elsevier.com/journal-of-economic-criminology

Deconstructing a form of hybrid investment fraud: Examining 'pig butchering' in the United States[☆]

Marie-Helen Maras^{a,*1}, Emily R. Ives^{b,2}^a Department of Security, Fire and Emergency Management and Center for Cybercrime Studies, John Jay College of Criminal Justice, City University of New York, 524 W. 59th Street, Haaren Hall, Room 43311, New York, NY 10019, United States^b Program in Cognitive Psychology, University of Virginia, United States

ARTICLE INFO

Keywords:

Pig butchering
Hybrid investment fraud
Cryptocurrency
Cyber-enabled crime
Cyber-enabled fraud

ABSTRACT

Cyber-enabled fraud has transformed, becoming more complex and making it harder for targets and law enforcement to detect its occurrence. This study aims to recontextualize a major manifestation of this transformation, a crime called hybrid investment fraud, colloquially known as pig butchering. Hybrid investment fraud describes a cyber-enabled fraud whereby criminals gain the trust of victims by forming connections and relationships, and then exploit this trust by using a series of confidence building and coercive measures designed to encourage victims to continuously invest in securities or commodities until they become unable or unwilling to continue to make payments or the offenders become unreachable. This study further aims to address the existing knowledge gap by focusing on understudied elements of this fraud, such victim and offender characteristics and the ways hybrid investment fraud is perpetrated. To achieve this, we conducted an in-depth analysis of more than 1,300 news articles and court documents between January 1, 2018, and November 1, 2023, to identify 59 cases of hybrid investment fraud targeting victims in the United States. This article both situates hybrid investment fraud within the broader fraud literature and conducts a comprehensive analysis of hybrid investment fraud cases to identify the types of hybrid investment fraud committed, their impact, victim and offender demographics, and offenders' tactics, tools, and methods of operation. The findings from this study can inform criminal justice practices and future research of this fraud.

1. Introduction

Online deceptive practices are perpetrated for various reasons. As Levine et al. (2010) identified in their study on deception, "people lie for a reason" (p. 272). While lying is not illegal, lies could strategically be used to facilitate the commission of a crime. The deceptive tactics used online are strategically designed with particular ends in mind, often, but not exclusively, financial in nature.

Countries all over the world have experienced cyber-enabled fraud, which involves the use of information and communication technology (ICT) to engage in illegal acts that result in a loss of property. A relatively new term that has been used to describe a specific form of cyber-enabled fraud in the United States is 'pig butchering.' According to the Financial Crimes Enforcement Network (hereafter FinCEN), this fraud

resemble[s] the practice of fattening a hog before slaughter. The victims in this situation are referred to as 'pigs' by the ...[offenders] who leverage fictitious identities, the guise of potential relationships, and elaborate storylines to 'fatten up' the victim into believing they are in trusted partnerships. The ...[offenders] then refer to 'butchering' or 'slaughtering' the victim after victim assets are stolen, causing the victims financial and emotional harm (FinCEN, 2022, p. 1).

While the term itself is not new in the country in which it originated – China (the term in Chinese is Shā Zhū Pán), it has recently become used with more frequency in U.S. news reports, court documents, and government publications. There is currently a dearth in academic literature studying this form of fraud, especially in the United States. This

[☆] Funding for this project has been provided by the Center for Cybercrime Studies, John Jay College of Criminal Justice, City University of New York.

* Corresponding author.

E-mail addresses: mmaras@jjay.cuny.edu (M.-H. Maras), xby5us@virgina.edu (E.R. Ives).

¹ ORCID: 0000-0003-3428-4622

² ORCID: 0009-0006-1494-5461

research seeks to fill this gap by engaging in an exploratory study of pig butchering incidents in the United States. Specifically, this article first situates the cyber-enabled fraud of pig butchering in the broader academic literature on fraud. It then conducts an in-depth analysis of court documents and new articles to identify the elements of this fraud, impact of the fraud, victim and offender characteristics, and tactics, tools, and methods of operation of offenders. The motivating research questions for this analysis are: Who are the offenders and targets in pig butchering? Is pig butchering committed by lone actors, dyads, or by organized criminal groups? What are offenders' tactics, tools, areas of operation, and modus operandi? The findings can be used to inform criminal justice practices and future research.

2. Fraud literature

Fraud is a crime that involves the use of tactics designed to misrepresent facts with the intention of persuading targets to provide offenders with something that is considered of value to the offenders. Fraud that involves the use of ICT to enhance and/or facilitate a fraud is known as cyber-enabled fraud. Offenders who engage in cyber-enabled fraud adopt various online personas, identities, and backstories to target individuals across demographics (Button and Cross, 2017). Frauds, including cyber-enabled frauds (i.e., frauds facilitated and enhanced by ICT) have evolved over the years, particularly perpetrators' tactics, targets, and methods of operation.

2.1. Cyber-enabled fraud

Cybercrime is frequently defined by taxonomies aimed at identifying and distinguishing features of crimes targeting and/or committed using ICT. There is no universal definition of cybercrime and no universally accepted taxonomy. Various definitions and typologies have been proposed (for a detailed review and critique of these typologies, see Sarkar and Shukla, 2023). Due to the breadth of crimes considered as cybercrime, Gordon and Ford (2006) proposed a continuum of cybercrime, whereby on one end, crimes only have peripheral technological aspects, and on the other end, crimes are entirely or "almost entirely technological in nature" (p. 3). Gordon and Ford (2006) divided cybercrime into two types - Type I and Type II. Type I includes cybercrimes such as "phishing attempts, theft or manipulation of data or services via hacking or viruses, identity theft, and bank or e-commerce fraud based upon stolen credentials," among others (Gordon and Ford, 2006, p. 2). Type II includes cybercrimes like "cyberstalking and harassment, child predation, extortion, blackmail, stock market manipulation, complex corporate espionage, and planning or carrying out terrorist activities online" (Gordon and Ford, 2006, pp. 2-3).

McGuire and Dowling (2013) view cybercrime as an "umbrella term" that includes cybercrimes that fall under two overarching categories: cyber-dependent crime and cyber-enabled crime (p. 5). Cyber-dependent crime includes crimes that target "the confidentiality, integrity, and availability of systems, networks, and data that would not be possible without the use of technology" (Maras, 2024, p. 9). Cyber-enabled crime is a term used to describe crime that is typically perpetrated in the physical world but is enhanced by "technological integration" and facilitated by technology (Sarkar and Shukla, 2023). McGuire and Dowling's (2013) categorization of cybercrime, which is based on the role of technology in crime, is most widely used. Europol (2018), Interpol (see Cross et al., 2021), and other national, regional, and international agencies and organizations commonly use these terms to broadly describe the acts of cybercrime based on whether the criminal acts would not have been possible without the advent of ICT (*cyber-dependent crime*) and whether the criminal acts represent traditional crimes that are enhanced and facilitated by ICT (*cyber-enabled crime*). The United Nations Office on Drugs and Crime (UNODC) also uses these cybercrime categories in documents (e.g., UNODC, 2022) and has used alternative categories of cybercrime, such as "acts against

the confidentiality, integrity and availability of computer data or systems" (i.e., cyber-dependent crime); "computer-related acts for personal or financial gain or harm" (i.e., cybercrime committed "for personal or financial gain or harm" (UNODC, 2013, p. 16); and "computer-content related acts" (i.e., cybercrime that "involve[s] illegal content"; UNODC, 2019) (see also UNODC, 2013). The latter two categories of cybercrime are considered subcategories of cyber-enabled crime.

By contrast, Wall (2007) proposed three categories of cybercrime: *computer integrity crime* (which encompasses cyber-dependent crime, such as hacking and distributed denial of service attacks); *computer associated crime* (covering cyber-enabled crime, such as cyber theft); and *computer content crime* (covering cyber-enabled crime, such as child sexual abuse material). The latter two categories are similar to the subcategories of cyber-enabled crime that UNODC used in 2013, "computer-related acts for personal or financial gain or harm" and "computer-content related acts," respectively (UNODC, 2013; see also UNODC, 2019). In his later work, Wall (2015) identified cybercrimes as occurring over a spectrum, with cyber-dependent crimes on one end of the spectrum and cyber-assisted crimes (i.e., crimes whereby ICT plays an incidental or ancillary role in the crime) on the other end of the spectrum. Between these two ends of the continuum are a range of cyber-enabled crimes (e.g., various forms of cyber-enabled fraud). In this work, he rightly pointed out that these categories merely described the "level of mediation of technology" and further differentiation was needed to identify the method of operation (modus operandi or M.O.) of offenders (Wall, 2015). For this reason, he identified the need to distinguish between *crimes against the machine* (i.e., cyber-dependent crimes), *crimes using the machine* (i.e., cyber-enabled crimes consisting of "computer-related acts for personal or financial gain or harm"), and *crimes in the machine* (i.e., cyber-enabled crimes that are "computer-content related acts"). Wall (2015) further noted that beyond the consideration of the M.O. of offenders, the victim group (i.e., nation state, business, or individual) targeted by the cybercrime needs to be considered as well.

Echoing Wall's (2015) sentiment for the need to create a more robust typology that moves beyond the role of ICT in crime, the development of cybercrime classifications based on offender motivation and intent have been proposed by various scholars who criticized Gordon and Ford's (2006) and McGuire and Dowling's (2013) cybercrime categories as employing "arbitrary attributes" (Lazarus et al., 2022, p. 384) and "obscuring the meaning of each cybercrime they represent" (Lazarus, 2019, p. 18, citing Ibrahim, 2016). To better understand the underpinnings and context of specific cybercrimes, which Lazarus (2019) argues serve as "a resource in understanding connections between gender and" cybercrime (p.19, citing Citron, 2014; Jane, 2016; Lazarus and Okorie, 2019), the Tripartite Cybercrime Framework (TCF) was created by Ibrahim (2016). This framework takes into consideration offender motivation that categorizes cybercrime into (Lazarus et al., 2022, pp. 385-386):

- *socioeconomic cybercrime* (i.e., "the computer or/and Internet-mediated acquisition of financial benefits by false pretense, impersonation, manipulation, counterfeiting, forgery, or any other fraudulent representation of facts such as online fraud");
- *psychological cybercrime* (i.e., "digital crimes that are primarily psychologically driven to cause shock, distress or harm to a person, where monetary gain is not the primary objective," such as cyberstalking, cyberharassment, and cyberbullying); and
- *geopolitical cybercrime* (i.e., "cybercrimes that are fundamentally political in nature and involve agents of the state...and/or their representatives engaged in acts;" for example, cyberespionage).

Ibrahim (2016) acknowledged that specific types of cybercrime could fit into two or three of the above-mentioned categories. Other scholars also acknowledge that the "apparent boundaries between the TCF categories are somewhat blurred" and thus the framework can be

viewed “as a loose grouping of cybercrime types” (Lazarus et al., 2022, p. 393). For example, image-based sexual abuse perpetrated using artificial intelligence (AI) manipulated media (e.g., deepfakes) can be perpetrated for a myriad of reasons, including personal, social, economic, and political reasons. The same holds true for fraud. The motivations for fraud vary by fraud type and offender. Even romance frauds, which have been predominantly associated with economic motivations in the literature, could be primarily psychologically motivated (e.g., catfishing where offenders primarily seek to form emotional bonds with others under false pretenses; not driven by monetary reasons) or geopolitically motivated (e.g., targeting politicians to impact elections; Michaelson, 2023). Like the aforementioned examples, hybrid frauds, which combine one or more types of frauds, do not necessarily fit neatly into one of these categories, unless the offenders are motivated for the same reasons (i.e., socio-economic, psychological or geopolitical).

Fraud, like cybercrime, is an umbrella term that encompasses numerous forms of illicit activities committed for a myriad of reasons against various victim groups. For this reason, to better understand pig butchering, we situate this cyber-enabled fraud in existing fraud literature.

2.2. Fraud taxonomy

The fraud taxonomy that is used to identify and classify fraud was created in 2015. This typology, developed by the Financial Fraud Research Center at the Stanford Center for Longevity and the Financial Industry Regulatory Authority (FINRA) Investor Education Foundation, classified fraud based on three elements (Beals et al., 2015). First, fraud is classified based on the target of the fraud: individual or organization. The fraud taxonomy only focuses on frauds committed against individuals. The second element of the taxonomy is expected benefit/outcome (i.e., the fraud category). Particularly, fraud committed against individuals is subdivided into several general categories of fraud: consumer investment fraud; consumer products and services fraud; employment fraud; prize and grant fraud; phantom debt collection fraud; charity fraud; and relationship and trust fraud (Beals et al., 2015). These general categories of fraud are further subdivided by the specific type of fraudulent item/transaction/relationship (i.e., the type of fraud). According to Beals et al. (2015), the seven general categories of fraud are considered “comprehensive and mutually exclusive, such that all possible examples of individual financial fraud committed against persons ... should fall into one and only one of the ...seven categories” (p. 11).

However, hybrid frauds do not fit neatly into one of the existing categories included in the fraud typology. One such hybrid fraud involves the convergence of romance fraud and investment fraud. Romance fraud is a form of fraud where offenders foster online relationships with victims “for the purpose of deceiving unsuspecting victims to extort money from them” (Coluccia et al., 2020, p. 25 cited in Cross, 2023, p. 2). Romance fraud, a subcategory of relationship and trust fraud that exploits a personal relationship with the target, has the expected outcome of creating a fake relationship with the target and exploiting this relationship (Beals et al., 2015). Offenders perpetrating romance fraud create fake online personas or profiles (complete with fake image and fraudulent personal narratives) and identify targets to engage in a tactic known as ‘catfishing,’ whereby offenders prey on targets’ desire for emotional connections and companionship (Whitty and Buchanan, 2016; Buchanan and Whitty, 2013), and lure them into fake relationships (Maras, 2017). The goal is often – but not always – to obtain something of value from targets (value, however, is determined by the offenders on an individual basis). In the United States, the forging of online romantic relationships is increasingly common (Wiederhold, 2020), which exposes individuals to various forms of romance fraud. Exposure to investment fraud is also quite common in the U.S. (Fletcher and Consumer Protection Data Spotlight, 2023).

Investment frauds are defined as “[d]eceptive practice[s] that induce... investors to make purchases based on false information. These ... [frauds] usually offer the victims large returns with minimal risk” (IC3, 2021, p. 31). These investments involve a range of commodities and securities. Several terms have been used to describe the convergence between romance fraud and cryptocurrency investment fraud, including pig butchering, cryptorom, and romance baiting.

2.3. Pig butchering

The range of frauds that are considered pig butchering vary by definition and origination. China, where the term pig butchering originated, considers it (Shā Zhū Pán) as

a form of online fraud, in which scammers gain the trust of victims through making friends and dating online. Through gaining victims’ trust, scammers then wait for the opportunity to pull victims into scams such as gambling or financial management to defraud their money. The biggest feature of Shā Zhū Pán is to cast a long-term plan for a major return. This process is like fattening pigs and then slaughtering them (China News, 2019, cited in Wang and Zhou, 2023, p. 915).

This definition was broader than the types of fraud identified in the 2021 Internet Crime Complaint Center (IC3) Annual Report as pig butchering. This report identified the incidents where victims reported being subjected to cryptocurrency fraud and ‘confidence/romance scams’ as pig butchering (IC3, 2021).

Other definitions also view pig butchering as involving the convergence of romance fraud and investment fraud, such as cryptorom and romance baiting. The term cryptorom “is an amalgamation of crypto- from ‘cryptocurrency’ and -rom from ‘romance scam’ (Ducklin, 2021; see also Chandriaiah and Wu, 2021)” (Cross, 2023, p. 5). In Australia, the term “romance baiting” is used to describe frauds that involve the convergence of romance fraud and investment fraud (Cross, 2023; Australian Competition and Consumer Commission, 2023). The Australian Competition and Consumer Commission’s (2023) definition of romance baiting describes it as originating from contact via online dating apps. According to their definition, the offender “initially contacts a victim via a dating app, then quickly moves the conversation to an encrypted chat site. After a few weeks of developing a relationship, the scammer will begin asking about the victim’s finances and encourage them to participate in an investment opportunity” (p. 32). However, hybrid romance fraud and investment frauds can originate outside of online dating apps. In fact, offenders look for and/or contact targets on social media platforms (Facebook/Meta, Instagram), professional networking sites (e.g., LinkedIn), dating sites (e.g., Hinge, Tinder, and OurTime), and communication platforms (e.g., WhatsApp, Telegram, and WeChat) (Access Wire, 2022; GASO, 2021b; FinCEN, 2023), as well as send unsolicited calls and/or text messages (SMS) to targets (see Image 1).

Targets may also be invited or added to groups and/or sent group messages on social media and communication platforms (GASO, 2021c) (see Image 2 for an example of a group chat invite). GASO (2021c)

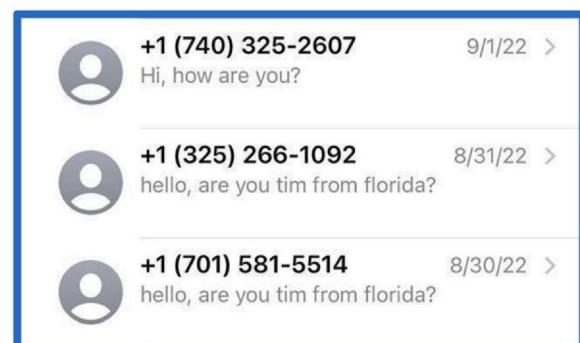


Image 1. Unsolicited text messages. Source: Authors.

Image 2 - Group chat invite

Image 2. Group chat invite. Source: Authors.

explained how frauds via group chat worked, where a fraudulent ‘investment lecturer,’ who claimed to be teaching those in the group chat how to invest effectively, engaged with victims in group chats. This ‘instructor’ used hybrid investment fraud tactics, with the added false sense of security of being in a group setting, to encourage investments under the guise of providing professional advice (GASO, 2021c). Usually, the purpose of these groups is to place targets in an environment that promotes offenders’ cryptocurrency investments. The offenders may even have multiple numbers, run multiple accounts, and/or have accomplices who answer targets’ questions and falsely claim to have positive experiences with the promoted cryptocurrency investment. These group chats are designed to be environments that make targets feel more at ease since they are led to believe that ‘others’ are also investing.

While the terms ‘cryptorom’ and ‘romance baiting’ emphasize the romance elements of the fraud, the original conception of pig butchering (*Shā Zhū Pán*) does not necessarily require that the relationships developed are romantic. The Australian Competition and Consumer Commission’s (2023) uses the term ‘relationship baiting scam’ to refer to investment fraud perpetrated by new online friends. The Global Anti Scam Organization (GASO), which was developed in 2021 in direct response to pig butchering outside of China, also highlighted that not all pig butchering instances describe frauds that began with a romantic relationship between a victim and offender (GASO, 2021b).

2.3.1. Impact of fraud

In the United States, cyber-enabled crime, including various frauds, are reported to the IC3. In 2021, IC3 received 24,299 ‘confidence fraud/romance scams’ reports with an estimated \$956 million in losses (IC3, 2021, p. 12). The following year, IC3 (2022) received 19,021 reports of this form of cyber-enabled fraud (Table 1). While there were fewer confidence/romance scams reported in 2022 than in 2021, the number of investment frauds increased that year (Table 1). In 2022, IC3 received 30,529 reports of investment fraud, having increased from 20,561 in 2021, and 8,788 reports in 2020 (see Table 1). The financial losses reported for investment fraud have exponentially expanded from more than \$336 million in 2020 to more than \$3.3 billion in 2022 (see Table 2). In 2021, IC3 reported that over 4,325 of the reports they received for confidence/romance frauds also included investment and cryptocurrency fraud (IC3, 2021, p. 12).

IC3 does not record pig butchering under the label ‘pig butchering’ in its reports and does not record hybrid romance fraud and investment fraud as a romance fraud and an investment fraud. Hybrid fraud, rather, is recorded based on the ends sought – that is, the ultimate goal of the hybrid fraud. Because the ends sought are investments, IC3 reports them as an investment fraud.

Specific financial losses for victims of pig butchering were provided in a couple of studies. Wang and Zhou (2023) identified the minimum

Table 1

Number of Confidence Fraud/Romance Fraud and Investment Fraud Reports Received by IC3 (2020–2022).

	2022	2021	2020
Confidence/Romance	19,021	24,299	23,751
Investment	30,529	20,561	8,788

Source: IC3 (2022).

Table 2

Financial Losses for Confidence Fraud/Romance Fraud and Investment Fraud Reported to IC3 (2020–2022).

	2022	2021	2020
Confidence/Romance	\$735,882,192	\$956,039,739	\$600,249,821
Investment	\$3,311,742,206	\$1,455,943,193	\$336,469,000

Source: IC3 (2022).

and maximum financial loss of the 40 victims identified from their online testimonials at an estimated maximum of \$410,000 USD and an approximate minimum loss of \$714 USD, and the four victims identified from police reports at a minimum of an estimated \$1500 USD and a maximum of approximately \$15,000 USD. GASO’s (2022) survey revealed an average loss of \$155,117 USD experienced by victims internationally (this amount excludes 38 cases where victims reported a fraud loss under \$2,500 USD) and average fraud loss experienced by surveyed victims from the United States was \$210,760 USD. GASO’s (2022) survey results further revealed that over 75% of victims in their sample reported losing “more than half their net worth,” while one third accumulated debt because of the fraud.

2.3.2. Victims and offenders

There is limited work that identifies offender and victim data and the average length of hybrid frauds. One study was conducted on Chinese victims who experienced Shā Zhū Pán. Data for this study was gathered from 40 online testimonials from Chinese individuals who experienced Shā Zhū Pán and posted about it on a forum, Zhihu. Their sample consisted of 36 women and 4 men. The victims’ relationship status included single (21), married (7), and divorced (3) (Wang and Zhou, 2023, p. 924).³ The victims’ online posts revealed that the shortest duration of the relationship between a victim and offender was 2 days, and the maximum duration was 8 months (Wang and Zhou, 2023, p. 924). The study also included four (4) police reported incidents of pig butchering. These cases involved three (3) women, one (1) man and a minimum and maximum duration of the relationship (min. 5 days; max. 29 days) (Wang and Zhou, 2023, p. 924). The age of the victims was not included in the analysis (as it was missing from the online testimonials).

The age group, gender, and relationship status of the targets of pig butchering have been identified in limited academic, governmental, and/or non-governmental works.⁴ In Australia, individuals under the age of 35 experienced “almost half of all reported losses to romance baiting” in 2020 (Scamwatch, 2021), which was comparable to findings in China, where victims in their “twenties and thirties” were the primary targets of the fraud (Zuo, 2021, cited in Cross, 2023, p. 6). GASO’s (2022) survey of 550 pig butchering victims from around the world revealed a relatively higher concentration of targets between the ages of 25 and 40. GASO’s (2022) survey sample included men and women, though women predominantly made up the sample (at 65%). The relationship status of the victims primarily targeted by pig butchering schemes were single (66%), followed by 21% who were married and 12% who were divorced/separated.⁵

The term ‘vulnerable’ has been used to describe the populations often targeted by perpetrators engaging in pig butchering. We use the term not only to include vulnerable age groups, such as the elderly, but also a wider range of individuals, including those who are emotionally

³ Some victims in the study reported their relationship status as uncertain (Wang and Zhou, 2023, p. 924).

⁴ IC3 data is not included here as IC3 does not distinguish between pig butchering and traditional investment fraud in victim and offender demographics.

⁵ GASO did not explain the missing 1% in the sample.

vulnerable (i.e., recently divorced or having marital/familial difficulties), medically vulnerable, and those who are technologically vulnerable (e.g., those who are not well versed in cryptocurrency). This term also includes those who are socially or geographically isolated and cannot facilitate interpersonal interaction through means other than social media. As “Sean Gallagher, a senior threat researcher at the security firm Sophos who has been tracking pig butchering as it has emerged over the past three years...[stated:] ‘They go after people who are vulnerable. Some of the victims are people who have had long-term health problems, who are older, people who feel isolated’” (Newman, 2023). Moreover, it is important to note that “the same types of stories and profiles used by romance fraud offenders,” which can be used in hybrid investment fraud, continue to be successful, indicating an inability to identify these schemes and an inability for targets to identify themselves as victims (Drew and Webster, 2024).

Nevertheless, victims of pig butchering may not be the only ones who are vulnerable. Specifically, government announcements, alerts, and press releases have stated that pig butchering is “largely perpetrated by criminal organizations based in Southeast Asia who use victims of labor trafficking to conduct outreach to millions of unsuspecting individuals around the world” (FinCEN, 2023, pp. 1–2; see also FBI and IC3, 2023). Further, a report by the United Nations Human Rights Office of the High Commissioner (2023) revealed that human trafficking victims are held in facilities that run online fraud operations in Southeast Asia and forced to engage in online fraud. These documents suggest that the perpetrators of pig butchering may also be victims of a crime and part of a vulnerable population.

2.3.3. Stages of pig butchering

Pig butchering transpires in stages. According to Wang and Zhou (2023), pig butchering occurs in three stages: pig hunting, nurturing/grooming, and pig harvesting (pp. 925–934).

- In the *pig hunting phase*, perpetrators identify victims to target. Wang and Zhou (2023) findings revealed that during this stage, perpetrators conduct research with the intention of planning out effective strategies to employ to reap maximum profit, including collecting background information before initiating contact and by inquiring more about the victim within their first few interactions.
- In the second phase, the *nurturing/grooming phase*, Wang and Zhou (2023) identified that perpetrators use pre-written scripts on relationship expectations and resonance techniques that are designed to increase the victim’s emotional dependence on the perpetrators. The use of pre-written scripts has also been identified in romance fraud. According to Lazarus et al. (2023), these scripts are frequently obtained “from underground forums” and “are categorized based on the age, ethnicity, and gender of the targets” (p. 13).

Wang and Zhou (2023) identified three “visceral influences” perpetrators target by using resonance techniques to increase the victim’s emotional dependence on the perpetrators, and ultimately, persuade them for eventual investment. These visceral influences are a target’s “desire to know a stranger show[s]... interest... in them (victims), desire to have a romantic relationship, and desire to be liked by someone with commonalities” (Wang and Zhou, 2023, p. 926). Tactics used to elicit the desired influences include “sharing fabricated personal life details,” “increasing the victims’ expectations of future romantic relationships,” and relating interpersonally to the victim (Wang and Zhou, 2023, p. 926). At this stage, the perpetrators discuss investments and introduce investment opportunities. Moreover, Wang and Zhou (2023) found that perpetrators will also elicit a higher degree of trust from the victim during this stage by invoking “authoritative figures” by way of professional or seemingly professional investment applications/websites and attributing knowledge to professional affiliations. This is similar to the techniques that perpetrators of romance fraud use to establish authority and credibility (Lazarus et al., 2023).

- In the final phase, the *pig harvesting phase*, perpetrators actively encourage victims to invest, often allowing them to invest on the offender’s behalf initially or providing a small allowance to begin investing, increasing their confidence and comfort with the process and technology. Wang and Zhou (2023) note that rewards are also used to positively reinforce a target’s behavior - particularly, their continued investment of funds.

Throughout the three stages, Wang and Zhou (2023) also found evidence of emotional manipulation by way of alteration in relational attitude or use of contrasting “representational redescription” techniques (i.e., changing tone of the conversation depending on the stage of the fraud) before and after investments are made.

Cross (2023), who focused her research on the convergence of romance fraud and investment fraud (i.e., romance baiting), applied Whitty’s (2013) “persuasive techniques model” that “outlines seven stages of romance fraud” and identified which stages are consistent with romance baiting (see , pp. 3 and 5). The seven stages of romance fraud identified by Whitty (2013) and covered by Cross (2023) are as follows:

1. *Motivated to find the ideal partner.* Perpetrators find a victim that is looking for a romantic engagement.
2. *Presented with the ideal profile.* Perpetrators present the victim with a fake and desirable profile.
3. *Grooming process.* Perpetrators use rapport building techniques to establish trust and confidence, ultimately grooming the victim.
4. *The sting.* Perpetrators make a financial request.
5. *Continuation of the scam.* Perpetrators continue the fraud and increase financial requests for various reasons.
6. *Sexual abuse.* Victims are sexual abused. According to Cross et al. (2022), this stage does not always occur.
7. *Re-victimization.* Targets may experience “recovery fraud,” a form of re-victimization from a different offender or different fraud (Button and Cross, 2017).

Cross (2023) pointed out that the initial stages of a romance fraud pertain to romance baiting. She specifically highlighted differences in the reasons for requesting money, where unlike romance fraud, requests for money are not premised on emergency situations (e.g., hospital expenses). Cross (2023) further pointed out that romance baiting was not only harder to detect and investigate than romance fraud, but also that ‘red flags’ were reduced with romance baiting by offering investment opportunities rather than asking for money directly.

Non-governmental and governmental organizations have also identified the stages of pig butchering. GASO (n.d.) also broke down pig butchering in various stages: *packaging* (i.e., perpetrators falsely represent themselves and gain the interest of the victim); *raising* (i.e., perpetrators build and invest time in the relationship with the victim while grooming them to invest); *killing* (i.e., incentives offered to invest money, victims attempt to withdraw their funds and are unable to do so, excuses are given as why payments are needed to obtain funds, and coercive measures used to get victim to invest); and the *killed* stage (i.e., often try to coerce victims into giving them more money that is ‘owed to them’ and ultimately block the victim). In the U.S., the FinCEN (2023) identified the following methods used by perpetrators of pig butchering: *initial contact with the victim* (to gain victim’s confidence and trust); *the investment ‘sales’ pitch* (convincing the target to invest); *the promise of greater returns* (accumulating victims’ funds); and the *‘point of no return’* (i.e., stealing the funds once a substantial sum or a target sum is received, and ultimately becoming unreachable and ceasing communications with the targets).

2.3.4. What’s in a name

The term pig butchering has been criticized both for its lack of sensitivity towards victims but also because it does not adequately

conceptualize the crime it aims to describe (Cross, 2023; Whittaker et al., 2024). In solidarity with Cross' (2023) assessment of the crudeness of the term 'pig butchering' and Whittaker et al.'s (2024) assessment of this term as degrading and harmful to victims, we argue against its continued use and propose the use of the term *hybrid investment fraud*, as it: 1) better represents the multifaceted nature of this fraud; 2) encompasses the ultimate goal of this fraud (i.e., investments), which is the way this cyber-enabled fraud is recorded in the United States by IC3; 3) uses the word fraud to describe the crime instead of the widely used 'scam' because a scam is, by definition, not a crime; 4) uses the term fraud to underscore the seriousness of the crime and not minimize or trivialize it (Lazarus et al., 2023); and 5) does not dehumanize victims by equating them to 'pigs' and what happens to them as a 'pig slaughter.' For these reasons, we will refer to 'pig butchering' as hybrid investment fraud hereafter.

3. Methods

3.1. Data sources

Hybrid investment fraud is a relatively new phenomenon and has not been reported on extensively. Thus, we cast a wide net to gather a robust data set. We triangulated several diverse sources to obtain the most complete picture possible about hybrid investment fraud. To achieve this, we reviewed news reports and court documents that described instances of hybrid investment fraud. We specifically examined documents between January 1, 2018, and November 1, 2023, as the colloquial term 'pig butchering' started to appear in online reports in 2018. To find documentation of hybrid investment fraud cases with victims in the United States, a private case law database (NexisUni) was used. On NexisUni, we used the following search terms: pig butchering; Shā Zhū Pán; Shāz Hū Pán; and a combination of the terms 'romance scam' and 'investment scam,' 'romance scam' and 'cryptocurrency,' 'investment scam,' 'romance scam' and 'cryptocurrency,' 'trust-based,' 'investment,' and 'scam,' 'cryptocurrency,' 'confidence,' and 'scam;' and 'crypto' and 'catfishing.' As two transliterations for "Shā Zhū Pán" were used in documents, both were searched for, as described above (however, we note the correct term is Shā Zhū Pán). Moreover, results were limited to content from North America and documents written in English. We reviewed the results from our searches, particularly examining news reports under the "news" section and court documents from the "briefs, pleadings, and motions" section of the platform. In the news results, "group duplicates" was turned on. We did not use any web scraping tools as NexisUni does not allow scraping as part of its terms of use. Utilizing this search process, we identified over 1,314 documents that contained combinations of our relevant keywords.

3.2. Data analysis

We reviewed 1,314 documents to identify cases of hybrid investment fraud. Our review was limited to incidents involving victims based in the United States, thus, any article that described hybrid investment fraud but included victims who lived outside of the U.S. were removed. We also removed documents that only provided warnings and tips to avoid hybrid investment fraud and any documents that did not have details about an actual case. To ensure intercoder reliability, the authors reviewed the documents separately, coded the cases separately (i.e., whether the case was a hybrid investment fraud or not), then reviewed their results together. We disagreed on 34 documents and discussed our respective coding to resolve these disagreements. Ultimately, we were able to identify 59 distinct hybrid investment fraud cases with victims in the United States that occurred between January 1, 2018, and November 1, 2023 (see Table 3). Of these incidents, we found court documents for 24 cases, and 35 cases from newspaper articles covering unique instances of hybrid investment fraud carried out on victims within the United States. For the cases we identified in

newspapers, we conducted clearnet searches to find supplemental information about these cases.

Once we identified 59 cases, we conducted a comprehensive qualitative case study analysis. This analysis was motivated by the following research questions: Who are the offenders and targets in pig butchering? Is pig butchering committed by lone actors, dyads, or by organized criminal groups? What are offenders' tactics, tools, areas of operation, and modus operandi?

We developed a codebook with our findings. This codebook included information about the type of fraud, loss associated with the fraud, length of the fraud, victim and offender, and the tools, tactics, and methods of operation of perpetrators of this fraud. To ensure intercoder reliability, the cases were coded and discussed to verify consistency and resolve any disagreements. The authors also reviewed the final coding and conducted a final quality check.

4. Findings and discussion

Our in-depth analysis of the cases in our dataset revealed variations in the type of hybrid investment fraud perpetrated, the impact of the fraud, victim and offender demographics, and the methods of operation, including the tools, and tactics perpetrators used to commit this cyber-enabled crime.

4.1. Type of hybrid investment fraud

Our cases revealed various complex, multidimensional frauds that do not fit within Beals et al. (2015) fraud typology, representing a departure from the one-dimensional conceptions of fraud in this typology, and demonstrating that certain frauds today do not fit neatly into singular categories as required by these designations. Instead, our findings revealed various forms of hybrid investment fraud.

One of these hybrid investment frauds involved romance fraud and cryptocurrency investment fraud. This finding is in line with the literature that identifies this form of fraud as the convergence of romance fraud and investment cryptocurrency fraud (Cross, 2023). Nonetheless, our dataset also included cases that did not involve romance fraud, where only friendships and/or professional relationships were developed. This designation differs slightly from the original conception of Shā Zhū Pán, but cases that are more in line with the original conceptualization were also represented. Specifically, our dataset included cases where the relationship fostered between a victim and offender was friendship, and cases that involved only a professional relationship. These cases illustrate the multidimensional nature of hybrid investment fraud, whereby contacts and connections are made to achieve the end goals - the maximum number of investments to obtain as much money as possible from the victim.

4.2. Fraud impact

The exact amount of the targets' financial losses was not always included in the cases in our dataset. In the cases where this information was included, the financial losses ranged from \$22,000 USD to 9.6 million USD. In the case of the smallest reported fraud loss, a man was defrauded out of \$22,000 USD by someone he met on the MeetMe dating app (C36, Sophos, 2023). The case with the largest amount of reported financial loss involved a victim who invested 9.6 million USD over four months on what they were led to believe was a legitimate cryptocurrency investment platform (C21). Most of our cases involved victims who invested hundreds of thousands of dollars, which is much higher than the average loss reported internationally (see, for example, GASO, 2022). While GASO (2022) reported an average loss for U.S. victims in the low hundreds of thousands USD, the cases we identified predominantly reported losses in the mid to high hundreds of thousands USD. Our dataset also included multiple cases where the fraud loss to victims was in the millions. While there were two cases (C44 and C40)

Table 3
Cases (*Full citations included in the reference list).

Case	Citation	Case	Citation	Case	Citation	Case	Citation	Case	Citation
C1	In the Matter of Application by the United States for Seizure Warrant, 2022.	C13	Leonard Terry Licht v. Tina Ling and Luxkey, 2023	C25	U.S. Attorney's Office and Central District of California, 2023 ^a	C37	Podkul, 2022 ^b ; Farivar, 2022	C49	Middle East North Africa Financial Network, 2022
C2	United States of America v. Approximately 1,360,000.748 Tether et al., 2023	C14	United States of America, v. 1. 12,324,84 USDT et al., 2023	C26	Kelly, 2023 ^{c*}	C38	Pawaon, 2023 ^b	C50	Falcon, 2022 ^{c*}
C3	United States of America v. Hailong Zhu, 2023a; United States of America v. Hailong Zhu, 2023b; United States of America v. Hailong Zhu, 2023c; United States of America v. Hailong Zhu, 2023d	C15	Commodity Futures Trading Commission, v. Cunwen Zhu and Justby International Auctions, 2023	C27	Kelly, 2023 [*]	C39	Middle East North Africa Financial Network, 2023	C51	Wang, 2021 [*] , ^d
C4	United States of America v. 5,012,294.90 in TetherUS et al., 2023	C16	State of Indiana v. Xu Xiongju et al., 2023	C28	Bartlett, 2023	C40	Lee, 2022	C52	In the Matter of the Seizure of Funds not to Exceed \$351,000.00 et al., 2022
C5	Gurung, Anjita v. Metaquotes et al., 2023	C17	United States of America v. Jin Hua Zhang et al., 2022	C29	In the matter of Cresttrademining Limited ^e	C41	Alabama Securities Commission, 2022	C53	In Re Bien, 2022
C6	United States of America v. 56,382,970.0 Tether et al., 2023	C18	OKX.com, Elaine Kim Chen Yu et al., 2023 ^f	C30	In the matter of Forex Market Trade, ^g	C42	Federal Trade Commission FTC, 2021 ^h	C54	United States of America vs. United States of America et al., 2023
C7	United States of America v. Approximately 503,349.86 Tether et al., 2022	C19	Adebayo, 2023	C31	In the matter of MetaCapitals Limited ⁱ	C43	Sophos, 2023b	C55	Albert ,Abed v. Wei Lin et al., 2023
C8	United States of America, v. 86,766.00 USDT et al., 2023	C20	Zimwara, 2023 ^j	C32	Armstrong, 2023	C44	Faux, 2023	C56	United States of America, vs. Zeshawn Stanley, 2023 ^{k*}
C9	Michael Bullock v. Jessica Doe et al., 2023	C21	In the matter of seizure of the domain names simexcbt.com et al., 2022; U.S. Attorney's Office, Eastern District of Virginia, 2022 ^k	C33	Sophos, 2023a ^l	C45	U.S. Attorney's Office, District of New Jersey, 2022 [*]	C57	U.S. Department of Financial Protection and Innovation, 2022a ^m
C10	In the matter of the seizure of up to 489,269.52 Tether et al., 2023	C22	Schoeff, 2023	C34	Podkul, 2022 [*]	C46	Lim, 2022	C58	U.S. Department of Financial Protection and Innovation, 2022b ⁿ
C11	Brian Hoop v. Emma Doe and John Does I-XX et al., 2023	C23	Owczarzak, 2023	C35	Podkul, 2022 [*]	C47	Allen, 2021	C59	U.S. Department of Financial Protection and Innovation, 2022c ^o
C12	Diyya Gadasalli v. Jerry Bulasa et al., 2022	C24	CE Noticias Financieras English, 2022b	C36	Podkul, 2022 [*]	C48	Roose, 2022		

*Court document of case used that the NEXISUNI news report mentioned details about or referenced.

^{**}More than one case included in the source.

^{***}Other document used based on information obtained from NEXISUNI news report (Sandhu-Longoria, 2023).

^aOther document used, which was found based on information from the NEXISUNI news report (Crypto Breaking News, 2023b; In the Matter of Seizure of any and all funds 2022).

^bOther document used, which was found based on information from the NEXISUNI news report (Anuforo, 2023).

^cOther document used about case NEXISUNI news report (CE Noticias Financieras English, 2022a) referenced.

^dOther document used about case NEXISUNI news report (Governance, Risk & Compliance Monitor Worldwide, 2023) referenced.

^eOther document used about case NEXISUNI news report (Governance, Risk & Compliance Monitor Worldwide, 2022a) referenced.

^fCourt document about case the NEXISUNI news report (U.S. Fed News, 2023) referenced.

^gOther document used about case NEXISUNI news report (Governance, Risk & Compliance Monitor Worldwide, 2023) referenced.

^hOther document used about case NEXISUNI news report (NEXISUNI news report (Podkul, 2022).

ⁱOther document used about case NEXISUNI news report (Governance, Risk & Compliance Monitor Worldwide, 2023) referenced.

^jOther document used about case NEXISUNI news report (Crypto Breaking News, 2023a) referenced.

^kOther documents used, which were identified based on information provided by the NEXISUNI report (Pepper, 2023).

^lMore information about this case was obtained from the original Sophos news report referenced in the NEXISUNI news report.

^mOther document used about case NEXISUNI news report (Governance and Compliance Monitor Worldwide, 2022) referenced.

ⁿOther document used about case NEXISUNI news report (States News Service, 2022b) referenced.

^oOther document used about case NEXISUNI news report (States News Service, 2022a) referenced.

where targets invested only \$100 USD, these cases were not included as the lowest amount of investment because the targets were journalists and knew they were being defrauded. For example, in one of these cases (C44), an investigative journalist followed the instructions of the offender and made a modest deposit only to learn more about how this fraud worked ([Faux, 2023](#)).

Our findings revealed significant financial losses that extended beyond the initial target of the fraud. In several cases, victims requested help from family and/or enlisted family and friends to ‘invest’ in the scheme. Victims invested their inheritance, savings and/or retirement money, borrowed from retirement investment accounts, liquidated stocks, refinanced, or obtained a second mortgage on their homes, used parents’ home as collateral for loans, as well as money obtained from banks in the form of loans, and borrowed private funds from family members (e.g., parents). In one case, a victim liquidated his own and his wife’s retirement accounts, obtained a second mortgage on their home, sold their rental home, and recruited five (5) friends to invest in the scheme (C4). The total investments from the victim, his wife, and his friends were about \$4.3 million USD. Nevertheless, like other forms of fraud ([Bilz et al., 2023](#)), the losses associated with hybrid investment fraud are not just financial. Some victims reported adverse psychological and physical consequences of the fraud, including suicidal thoughts, psychiatric distress, admittance to hospital and/or emergency room, and the dissolution of and harm to interpersonal relationships (e.g., separation and/or divorce after fraud revealed and harm to relationships because they enlisted family and/or friends to invest in schemes). These results are consistent with those found in meta-analyses examining the outcome of romance fraud as several studies cite victim reports of “shame, embarrassment, shock, anger, worry and stress ([Whitty and Buchanan, 2016](#))” that “can be associated with subsequent physical and mental health problems... ([Cross, 2019](#))” ([Bilz et al., 2023](#), p. 8). While monetary loss is often a focus of legal intervention, emotional devastation frequently compounds the effects of various forms of cyber-enabled fraud.

4.3. Offenders and victims

4.3.1. Offender demographics

Offender gender demographics were not included for all offenders in all cases in our dataset. This information predominantly denoted the gender of offenders’ online personas rather than their real identity (except for offenders who were identified in court documents by their real names). Where gender identity related information was included (gender and gender pronouns included and/or offenders identified), we observed that offenders predominantly pretended to be a woman and targeted a man, or an offender pretended to be a man and targeted a woman. This tactic, known as gender swapping, is used to encourage the development of a romantic relationship and a reported manipulation tactic in romance fraud studies (see, for example, [Lazarus et al., 2023](#)).

Many cases identified at least one offender - either their real name or the fake name they used for the fraud, the person who contacted the victim, formed a relationship with the victim, and convinced and pressured the victim to invest in an opportunity. However, this does not necessarily mean that only one offender was involved in the fraud. Many of the cases mention a customer service representative, broker, account manager, platform administrator, support, or other contact from a fraudulent investment company. Certain cases also mention others, such as contacts or relatives who offer investment assistance to the victim at the request of the person who initiated contact with the victim; however, this does not necessarily mean that more than one person was communicating with the victim. We did not have complete data in most of the cases in our dataset to identify the number of offenders involved in the fraud (e.g., the same offender could have potentially initiated contact with the victims and served as the customer service or other representative from the investment platform). Court documents provided more robust information than the news articles,

but some of the documents involved civil actions where offenders were not named. In certain cases, the number of offenders were identified (though not always with the names of offenders). For instance, civil court documents named individual defendants as Jessica Doe (C9), John Does (C9, C11), Emma Doe (C11), and Does (C18).

Our dataset also identified the existence of organized criminal groups, which are defined as “a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offenses established in accordance with ...[the UN Convention Against Transnational Organized Crime (UNTOC)], in order to obtain, directly or indirectly, a financial or other material benefit” (Article 2(a), UNTOC). In our dataset, words such as ‘enterprise,’ ‘syndicate,’ or group were used to identify the involvement of three or more persons in the fraud. For example, the word ‘syndicate’ was used to describe groups engaging in hybrid investment fraud (C3) and groups engaging in hybrid investment fraud have been accused of running criminal enterprises (C5) and engaging in a “pattern of racketeering activity” (C16, p. 183). In one case, 11 members of the group were mentioned, each with their own roles in facilitating or assisting the hybrid investment fraud, committing wire fraud, money laundering, bank fraud, passport fraud, identity theft and other criminal activities (C17). In this case, we identified a familial connection between perpetrators - two brothers ran their hybrid investment fraud operation out of New York and New Jersey ([United States of America v. Jin Hua Zhang et al., 2022](#)).

Moreover, our dataset revealed organized criminal groups operating in concert to commit hybrid investment fraud. Specifically, one case (C15) identified three groups operating together to commit this cyber-enabled crime: *solicitors* (i.e., contacted victims, formed relationships, and convinced them to invest); *trading firms* (i.e., opened trade accounts on behalf of victims); and *shell companies* (i.e., accounts used to obtain fraud and misappropriate funds from victims). Solicitors pretended to be experts with insider knowledge and contacts that helped them be successful traders and introduced victims (known as “scheme customers”) to trading firms. Trading firms directed scheme customers to download fraudulent apps, and victims and others transferred money (for investment, fees, taxes, or other reasons) to shell companies.

Our dataset further revealed fraudulent companies, which played a role in the hybrid investment fraud. For instance, the New Jersey Bureau of Securities ordered three companies to cease and desist operations as they were found in violation of the state’s securities laws for their involvement in hybrid investment fraud schemes (C29, C30, and C31). Furthermore, in certain cases, companies were listed alongside individuals as defendants (e.g., C9 and C11).

The offenders were located both in the United States and abroad. In one case, one group was identified as operating in the same area in the United States ([United States of America v. Jin Hua Zhang et al., 2022](#)). Another case identified an organized criminal group made up of Chinese and Namibian nationals that targeted U.S. victims operating in Namibia (C20). In other cases, perpetrators stated they were and/or were believed to be in Canada, Cambodia, China, Laos, Thailand, Malaysia, and Vietnam. Countries in Southeast Asia have been identified in government documents as source countries for hybrid investment fraud ([FinCEN, 2023](#)) Particularly, in one case (C4), cryptocurrency exchange accounts identified in the fraud were registered from countries where hybrid investment fraud schemes originate (i.e., Thailand and Malaysia) ([United States of America v. 5,012,294.90 in TetherUS et al., 2023](#)). Reports have shown that human trafficking organizations in Cambodia, Laos, Thailand, and Malaysia have forced trafficked victims to conduct hybrid investment fraud ([Keaton, 2023](#)). Nonetheless, in many of our cases, the real and/or perceived actual location of the offenders was not identified.

4.3.2. Victim demographics

Predominantly, the names and demographic information of victims were not included. Many cases included initials of victims instead of

Table 4

U.S. States where victims are located.

Alabama	Michigan
Arizona	Minnesota
California	New Jersey
Colorado	New York
Connecticut	Ohio
Delaware	Pennsylvania
Illinois	South Carolina
Indiana	Tennessee
Iowa	Texas
Georgia	Virginia
Maryland	Washington
Massachusetts	Wisconsin

their names to protect their privacy. In those cases, we were only able to identify gender based on the pronouns used. Where gender information about victims was included, the number of victims that were men were more than double the number of victims that were women. Only thirteen (13) cases identified the age of the victim. The ages identified in these cases ranged between 20 s and 60 s: ages 22 (C47), 24 (C50), 33 (C48), 37 (C28), 41 (C27), 42 (C26), 46 (C46), 52 (C37 and C51), 61 (C2), 62 (C1 and C32), 68 (C18). The ages identified in our cases differed from the victim age group of hybrid investment fraud that the Global Anti Scam Organization (GASO) identified: ages 25–40. Only a couple of cases included words relating to age groups (i.e., ‘retired’; C25) and/or age ranges to identify the relative and/or approximate age of the victims (i.e., age range of 30 – 39; C42). When the relationship status of a victim was provided in the case documents, victims in the cases were identified as single, married, divorced, and/or widowed. Further, our dataset, which focused on U.S. victims, revealed that the victims were from various U.S. states (see Table 4).

Certain cases included information about the employment of victims. In these cases, the victims who were targets of this cyber-enabled fraud included (but were not limited to) a lawyer, life coach, trade manager, investigative journalist, technology executive, software engineer, marketing executive, financial advisor, real estate agent, hiring manager, business owner, and caretaker. Our dataset also revealed that vulnerable populations were targeted. Specifically, in our dataset, we identified victims who were emotionally vulnerable (e.g., isolated, loss of a loved one, recently divorced, or having marital/familial difficulties), medically vulnerable (e.g., long-term health problems and terminal diseases), and those who were technologically vulnerable (i.e., those who are not well versed in cryptocurrency and investing cryptocurrency). For example, when one victim met the perpetrator, she had been diagnosed with terminal cancer and was getting a divorce after 16 years of marriage (C24), another had lost his wife of 40 years to cancer (C13). In another case, an elderly woman suffering from early onset dementia and multiple sclerosis became the target of a hybrid investment fraud (C52). In addition, one victim was a political refugee from Nepal, who came to the U.S. because she was targeted by the Communist Party of Nepal (C5). This victim struggled with severe health issues from her loneliness and separation anxiety from her family, who were still in Nepal and experiencing threats and violence. Moreover, a hearing-impaired immigrant, who fled Iran because of religious persecution, became a target of this cyber-enabled fraud (C55).

4.4. Hybrid investment fraud stages: Offenders' M.O

Our dataset revealed that hybrid investment fraud includes various stages: approaching the target; cultivating a relationship with the target; discussing and promoting investments; getting victims to invest; and revealing the fraud. In what follows, we identify the stages and the tools and tactics used by offenders in each stage.

4.4.1. The approach

At this stage, like FinCEN's (2023) “initial contact with the victim” stage, a target receives an unsolicited call, message or connection

request and a connection is made between the target and the offender. Our dataset revealed that various forms of telecommunications and electronic communications were used to send unsolicited communications to targets. In the cases in our dataset that included this information, targets were first contacted by offenders via text messages (SMS) or calls; communications platforms (i.e., WhatsApp, Telegram, and Line); through social media platforms (i.e., Twitter, LinkedIn, Facebook/Meta, Snapchat, and Instagram); on online dating platforms (i.e., Tinder, Hinge, MeetMe, and Zoosk); and other online platforms (i.e., Homesnap, Airbnb, Hello Talk, and Tandem). Two language apps, HelloTalk and Tandem, which were designed to connect individuals seeking to improve language skills, were identified in our dataset as platforms individuals may repurpose and use to connect romantically.

The way offenders approached targets varied by the type of telecommunications and electronic communications used. When the methods used to connect to targets were calls, texts, and messaging applications, offenders used various excuses to explain why targets were contacted. These unsolicited communications often occurred under the pretext that offenders accidentally contacted them, were reaching out to someone they purportedly knew, or were reaching out pursuant to the direction of a third party. For example, in one case with multiple victims (C25), one of the victims was contacted via text message by a Chinese woman claiming that her mother supposedly encouraged her to contact him for the purpose of discussing marriage. On dating and social media platforms, offenders connect with targets under the guise of forming relationships, friendships, and/or professional connections. A couple of our cases involved offenders contacting targets to request a service they were providing (e.g., life coaching services, real estate assistance, and short-term rental assistance).

Initial contact also occurred in online group chats. In our dataset, one victim, while participating in a group chat on Twitter, was introduced to a fraudulent trading platform, known as Bitkam (C54). FINRA (2024) recently published an alert about fraudulent investment groups on social media. Individuals posing as legitimate investment advertisers are giving investment recommendations in these groups, which start on social media platforms and then often move their communications to encrypted communications platforms (e.g., WhatsApp) (FINRA, 2024).

Following initial contact, most cases in our dataset revealed that offenders encouraged communications to continue off social media and online dating platforms to other messaging platforms (e.g., WhatsApp, WeChat, Line, Skype, and Telegram). Victims are encouraged to move off social media and dating platforms as these platforms have algorithms that could detect suspicious and fraudulent activity. For example, the Match Group, which includes dating apps, such as Match, Hinge, Tinder, and Our Time, among others, has measures in place to help users identify fraudsters and fraud, by, for example, having user verification tools on their platforms, urging users to keep communications on the platforms and to use existing verification tools, sending messages and alerts to users with online safety dating tips, and using machine learning to identify fraudulent accounts based on activity (Skores, 2023; Goode, 2023). Nevertheless, these platforms are still used to initially engage the victim, and then move communications off these platforms to avoid detection of the fraud and deletion or blocking of their accounts.

4.4.2. Cultivating the relationship

Once a connection is made, the perpetrator initiates conversation to ultimately build rapport, trust, and a relationship with the target. At this stage, the offenders adopt various storylines and personas to successfully cultivate a relationship with victims. In our dataset, the offenders posed as entrepreneurs, asset managers, cryptocurrency investors or traders, employees at technology companies, architects, and business owners in the United States and abroad (e.g., a wine trader in France). The offenders claimed to have made money from investments and have expertise in cryptocurrency investments or gold trading.

Furthermore, one offender in our dataset fraudulently posed as a military veteran (C56).⁶ Fake personas that include persons of authority or credibility, like military members, are used to gain the victim's trust (Cross and Holt, 2021; Lazarus et al., 2023).

When offenders' profiles on online platforms and apps included pictures and/or offenders shared images with the targets, the offenders used images of attractive men and women and displayed wealth. The use of seductive images and visual portrayal of wealth are also common tactics used in romance fraud more generally (Bilz et al., 2023; Lazarus et al., 2023). The offenders' affluent lifestyles were purportedly made possible by their investments in securities and/or commodities. A couple of the cases revealed storylines where the offenders claimed to be Ivy League educated (e.g., Harvard University and University of Pennsylvania). An offender in one case posed as a graduate from the University of Pennsylvania, with expertise in gold trading and a history of extremely successful real estate and financial investments (C25).

Offenders in our dataset feigned empathy for victims experiencing hardships and provided emotional support. In one case, the offender connected with the victim by consoling him over his father's deteriorating health and placement in hospice (C37). Other offenders cited personal hardship as the reason for investing in commodities. For example, in one case, the offender, posing as a man, told the target that when his family business closed during the COVID-19 pandemic, he turned to cryptocurrency investments for income (C24).

Additionally, offenders in our dataset sought to establish personal bonds with victims and develop stronger connections with them. To do so, offenders frequently furthered false emotional connections with victims by incorporating shared trauma into newly developed narratives, or by establishing common personality traits, aimed at solidifying their relationship. This tactic is like what is described by Whitty (2013) in the "grooming process," GASO (n.d.) in the "packaging" and "raising" stage, and Wang and Zhou (2023) in the "nurturing/grooming" stage. Specifically, what we observed was the use of persuasion techniques (i.e., resonance techniques), such as "liking and similarity" to groom the victim (Wang and Zhou, 2023, p. 926). For example, in one case, the victim stated: "He looked very legitimate, started talking business with me, knew the company I work at. He had a friend who went to the same university as me years ago, and so we really connected that way" (C46). Persuasion techniques such as "visceral appeals, the creation of urgency, fast-moving relationships, appeals to strong emotions and even isolation and monopolization" are often used alongside linguistic devices to distract and disguise criminal intent from the victim by pushing clues indicating fraud to the periphery of the victims' thoughts and forefronting a connection and relationship (Bilz et al., 2023, p. 12).

We also identified the use of other resonance techniques identified by Wang and Zhou (2023) in their study. More precisely, offenders shared false personal information and experiences with victims. For instance, in one case (C35), an offender feigned a similar situation to the victim who informed him that she had a brother with special needs that she cared for (i.e., cerebral palsy), while in another (C48), the offender claimed to be from the same province in China as the victim's birth family, even going so far as to jokingly claim that they are siblings.

4.4.3. Making the 'case' for the investment

In this stage, the offender turns conversations towards investments. The offender then discusses expertise and/or prior success with investments. The goal of these conversations is to introduce the target to a lucrative investment opportunity, and then entice them to invest (which is the next stage). This can be likened to the FinCEN's (2023) "investment 'sales' pitch" stage and Wang and Zhou's (2023) "nurturing/grooming phase," where the investments are discussed, and investment opportunities are introduced and encouraged.

⁶ In the case, the offender predominantly engaged in romance fraud (except for one case of hybrid investment fraud).

4.4.3.1. Securities and commodities. Real and fake securities and commodities and associated technologies are the primary tools offenders, co-conspirators, and/or associates use to commit hybrid investment fraud. These tools are used by criminals to further their illicit ends and launder the proceeds of their crimes. Our dataset revealed the use of cryptocurrency for these purposes. Specifically, offenders encouraged victims to purchase cryptocurrencies, such as Binance Coin (BNB), Bitcoin (BTC), USD Coin (USDC), Tether (USDT), and Ethereum, and deposit them into accounts, apps, and/or online platforms, controlled by the offender(s) and/or associates. Offenders also directed victims to purchase/invest in Decentraland's virtual world cryptocurrency, such as Mana (C4). Nevertheless, not all investments in our dataset involved cryptocurrency. Unlike existing work that reduces hybrid investment fraud to frauds that involve cryptocurrencies, our dataset revealed five (5) cases where victims were not directed to invest in cryptocurrencies, but instead were directed to invest in a commodity, gold. In one case (C36), the victim fostered a romantic relationship with a man claiming to make money in the gold trade and asked him to teach her about this trading. The perpetrator taught her how to invest using MetaTrader – a fake brokerage. Other cases (C25, C42, C43, and C55) similarly involved the same fake brokerage.

4.4.3.2. Length of fraud. The length of the fraud was not always clearly delineated in the cases in our dataset. In the cases where the length of fraud was included, it was variable. Our dataset showed that some frauds lasted a little over a month until about six months (from initial contact to the ceasing of communications between victim and offenders), while other cases lasted much longer. This does not exactly reflect Wang and Zhou's (2023) findings, but also does not drastically differ from them. Moreover, it is possible that lengthier frauds are reported with more frequency. The lengthiest fraud in our dataset lasted for over two years (C5). In this case, over the course of two years, an unidentified offender (John Doe) convinced Anjita Gurung (a caretaker who was a native of Nepal living on the North Coast) to invest about \$597,000 USD.

The amount of time between the offender initially contacting the target to the time it took to switch to friendly, professional, or romantic conversations to discussions of investment opportunities also varied. In one case (C22), "[a]fter a couple of days of communicating, the suspect started to ask questions about the investor's financial background and investing habits" (In the matter of: www.batcipe.vip, James Yeh, www.batnap.vip, Kenju Go, 2023), while in another case (C46), the offender and the target were communicating for only two weeks before the conversation turned towards investments. In another case (C1), after matching on a dating platform and moving their conversations the same day, the offender, within five hours of communicating switched conversations to cryptocurrency, by "stat[ing], in an inorganic way to explain a five-minute delay in her response, 'Sorry, I was just analyzing the cryptocurrency blockchain market with my teacher'" (In the Matter of Application by the United States for Seizure Warrant, 2022, p. 10). What was consistent throughout the cases in our dataset was that, despite the variation in the length of time between initial contact and discussion of investment opportunities, the speed of this stage of the hybrid investment fraud was relatively slow (with a few exceptions) – at least when compared to the next part of the process, which involves the target's investment.

4.4.4. The fraudsters' toolkit for investments

At this stage, the offender exploits the relationship and uses a series of confidence-building techniques to gain the target's trust in the investment and/or coercive techniques to get the offender to invest and/or continue to invest. This stage is equivalent to GASO's (n.d.) "killing" stage, FinCEN's (2023) "promise of greater returns" stage, and the "pig harvesting phase" of Wang and Zhou's (2023).

4.4.4.1. Confidence building measures. In a handful of the cases, victims described measures taken by perpetrators to establish confidence in

their relationship and investment opportunities. These confidence building tactics ranged from offering financial assistance to victims for investments, to feigning insider knowledge of and connections to investment platforms, to providing false documents and information verifying and authenticating investments and investment platforms, to promoting the illusion that victims have control over their funds, to educating the victims.

4.4.4.1.1. Offers of financial assistance. To encourage further investments, certain offenders even offered to contribute money to victims' investments so victims can reach a higher investment goal and/or when victims could not invest more money and/or could not obtain all the funds requested by the platform to withdraw their funds. This is unique to hybrid fraud as this action is only possible due to the trust established by the intimacy of interpersonal relationships and the tactics used in investment fraud. In one case (C42), the offender offered to co-deposit money into the victim's trading account (she was told to deposit \$410,000 USD to her account and he claimed we would deposit \$700,000 USD to her account). In the cases where offenders purportedly financially contributed to victims' investments, they requested money from victims for personal expenses and demanded more investments from victims, and the investment platforms notified victims that third parties were not allowed to contribute to victims' investments and financial and personal information from these contributors was needed to verify the lawfulness of the transactions (i.e., to rule out money laundering). In the cases where the fraudulent investment platforms notified the victims of the issues associated with third party contributions, the victims had their accounts frozen and/or were charged fees as a penalty and for other reasons.

4.4.4.1.2. Insider knowledge and connections. Some offenders claimed to have insider knowledge and connections. In several cases, offenders who promoted investment opportunities to victims pretended to have a familial connection, most frequently an uncle, to the investment platform and/or someone with expertise in investment trading. In one case (C55), an uncle was mentioned during the initial interactions ("only child and lucky to have a great uncle who treats her as his biological daughter" p. 2). This initial introduction made the segue into later discussions about her uncle's connections to investment claiming that he is a "senior financial analyst at Blackstone Group and had been giving her financial advice" (p. 2). In another case (C4), the offender, who used a female persona ('Gracie'), claimed her uncle had a direct relationship with the management of the cryptocurrency exchange platform (NTU Capital) to encourage the victim to open an account there. Moreover, another offender in our dataset mentioned that her uncle, who ran an investment analysis team, would inform her of trades she should make (C25). Similarly, a victim in Wang and Zhou's (2023) dataset revealed that an offender mentioned an experienced uncle who taught him how to invest and conduct the requisite "financial statistical analysis" needed to profit from investments (p. 929).

Other cases identified relatives as having insider information and contacts within investment platforms. In one case, an offender with a female persona claimed to have an uncle that could obtain insider information about trading (C59). In another case (C9), an offender named Jessica told the victim that she had a godmother, who was "a purported insider and analyst at an options trading firm," and provided her with information that helped her successfully trade cryptocurrency options (p. 7). Apart from cases that revealed a familial connection, an offender from a case in our dataset (C25) claimed her best friend served as the Chief Financial Officer of the investment platform.

In their study, Wang and Zhou (2023) found that fraudsters "appeal to individual figures that have authoritative backgrounds, such as a family member working in a financial sector or an investment mentor, who either teaches fraudsters the investment skill or informs them how to earn quick money" (p. 929). These connections with 'authoritative figures' help build trust in the offender, the platform, and the investment process (Wang and Zhou, 2023).

4.4.4.1.3. Fake supporting documentation. In the cases we gathered for this study, we identified cases where offenders procured fake financial information and documents (including fake financial charts)

to establish legitimacy of false narratives, which were shared to inspire confidence in investment opportunities (e.g., C46; Lim, 2022). For example, perpetrators often falsely depict invested funds increasing on fake online platforms and apps or via screenshots.

4.4.4.1.4. Control over funds. In several cases in our dataset, victims could withdraw some of their deposited funds from their investments, at least initially. In another case, one victim mentioned that in order to test his control over funds he invested (and to check the legitimacy of the platform), he withdrew money and then deposited it again in his 'investment' account (C23). To this victim and others in our dataset, the success of this test (or tests, as certain victims were able to make more than one withdrawal) alleviated concerns and served as proof of the app and/or platform's legitimacy. This is similar to the tactic Wang and Zhou (2023) describe where perpetrators ask victims to make initial investments on their secondary accounts to inspire victim confidence and reinforce their perceived control over the situation. This method also contributes to another related tactic that perpetrators employ; educating victims on investment (see next section).

4.4.4.1.5. Served as teachers. A comfort level was established with investing to encourage victims to invest more over time. This was achieved by offenders offering to teach victims how to trade. Offenders walked victims through the process of investing (e.g., by providing screenshots of their screens or assisting them through video) and in limited cases, if assistance was needed, offenders requested remote access to victim devices to register them, registered virtual currency service provider or virtual asset provider accounts on behalf of the victim, and took control over the victim's account and/or made the investments on the victim's behalf. In one case (C9), the offender sent "screenshots of her phone with boxes (made using a hand-drawn feature to superimpose lines and shapes onto photos and screenshots) showing [him] which buttons she wanted him to click" (Michael Bullock v. Jessica Doe et al., 2023, p. 10). Offenders also walk certain victims through the successful withdrawal of some money they invested to show that the site or platform can be trusted.

Perpetrators provided education regarding cryptocurrency to build a false sense of financial literacy, which they could then exploit. An example of this tactic was seen in cases where perpetrators encouraged victims to invest using Tether, because it was a 'stable coin', meaning that this cryptocurrency had a more stable value. This trust in the cryptocurrency used imbues victims with confidence to invest in high-risk markets without considering other risks associated with new investments, including potential fraud.

4.4.4.2. Love bombing. Love bombing, which involves overwhelming a person with attention, affection, and constant communication via call, messages, emails, and other forms of communication, is another tactic that may be used by an offender in hybrid investment frauds. In the cases where romantic relationships (albeit false) are cultivated between victim and offender, the offender rapidly professes their love for the victim and discusses major life events with them, such as marriage and children. In one case (C1), the offender professed her love for the victim in less than 24 hours of initial contact. The purpose of the use of this tactic is to create a connection with and dependency on the offender to enable the offender to engage in manipulation and control tactics. In one case of love bombing (C40), the offender immediately started to engage in love bombing through repeated flattery and the sending of romantic messages. In another case (C2), one offender, who professed love for the target only after two days of communicating, demanded that the victim delete the messages of the perpetrator and the link the offender provided to the fraudulent investment application to prove that the victim was dedicated to him, thus forcing a more intimate connection between the two, through a display of devotion.

4.4.4.3. Threats. Offenders in our dataset used coercive measures to establish relationships and pressure victims to invest and provide additional funds to their original investments. When victims could no

Table 5

Examples of types of taxes, fees, penalties, and other charges to withdraw funds.

account guarantee	risk deposit fee
annual fee encumbrance	risk verification fund
blockchain congestion	security deposit
capital verification	service fee
credit enhancement guarantee	transfer funds
expediting the withdrawal	unfreeze account
margin loan fee	verification
management review	VIP member
profit tax	withdrawal fee
reflection fee	withdrawal processing

longer invest funds and/or obtain the necessary amounts needed to pay fees, penalties, taxes and/or other charges (see Table 5), the victims were threatened with the loss of the entire amount of their investment, further fees, freezing of their account, and/or criminal prosecution (i.e., for insider trading or money laundering). In one case with multiple victims (C25), one of the victims, after seeing profits on the platform, attempted to withdraw money from the account. A ‘representative’ from the platform notified the victim that money could not be withdrawn. In particular, the victim was notified that his account was frozen because the platform believed that some of the transactions of the victim might be illegal. The victim was informed that to lift the freeze on the account he had to pay 15% of the amount in the account to have the account reviewed. The victim was also informed that if he did not pay this money his account would be terminated. Furthermore, the victim was informed that nonpayment would result in his blocklisting and reporting to financial institutions and banks around the globe. In another case, an offender threatened to harm the victim’s consumer credit score (C9).

Certain offenders who fostered relationships with victims engaged in intimidation tactics, verbal abuse, blackmail, and threats of physical violence and harm. In one case (C11), when the victim refused to pay more money, the offender (who identified as ‘Emma’) became furious, attempted sextortion (i.e., threatening release of intimate messages and images if remuneration not provided) and informed the victim that she hired people to kidnap and torture him and have his organs harvested. Similarly, in one case (C5), after investment payments were terminated, the victim was harassed with threatening and sexually vulgar telephone calls via Viber and Telegram, aimed at encouraging her to reinstate her payments or to punish her for refusing to engage further. Such fear and intimidation are cited as common tactics used to coerce targets into complying with offenders’ demands (Buchanan and Whitty, 2013; Carter, 2020; Lazarus et al., 2023).

4.4.4.4. Tactics to obscure the fraud. There were several tactics used by offenders to obscure the fraud, making it harder for victims to identify the fraud. In most cases that involved cryptocurrencies, victims were directed to legitimate cryptocurrency exchanges (e.g., Binance, Bitstamp, Coinbase, Crypto.com, Gemini, Kraken, OKX, and Poloniex) to create a cryptocurrency account, and then directed to investment apps and platforms controlled by offenders. The actions taken thereafter were designed to confuse targets and trick them into providing offenders with control over the cryptocurrency account and/or transferring money to accounts, platforms or apps controlled by offenders.

One of the tactics identified in the dataset was domain spoofing, which is used to trick targets into downloading apps and/or accessing and using fraudulent websites designed and controlled by offenders. The spoofed website is designed to convince individuals that the site is legitimate and trustworthy, but it is actually a fake domain masquerading as a legitimate domain. For example, the spoofed website, by-bit.us, which the victim was directed to, mimicked the legitimate cryptocurrency exchange site Bybit.com (C18). To appear authentic,

spoofed websites also falsely claim to be award winning, affiliated with the legitimate cryptocurrency exchanges, U.S. Financial Crimes Enforcement Network (FinCEN) compliant, and regulated by the “United States (sic) Money Services Business” (see, for example, C4, United States of America v. 5,012,294.90 in TetherUS et al., 2023).

With a few exceptions in our dataset, targets did not have prior history, knowledge, or experience with the securities and commodities investments promoted by the offenders. Our dataset included cases where the investment promoted was liquidity pool mining, which is a legitimate but complex trading process. This form of mining works as follows:

A liquidity pool is a crowdsourced pool of cryptocurrencies or tokens locked in a smart contract that is used to facilitate trades between the assets on a decentralized exchange (DEX). Instead of traditional markets of buyers and sellers, many decentralized finance (DeFi) platforms use automated market makers (AMMs), which allow digital assets to be traded in an automatic and permissionless manner through the use of liquidity pools. Crypto liquidity providers are incentivized by earning trading fees and crypto rewards (new cryptocurrencies which can in turn be traded for other cryptocurrency or fiat currencies) (Seizure warrant, REACT Case #RT-2205-06106).

Victims’ limited knowledge of this form of investment was leveraged by perpetrators to engage in hybrid investment fraud. In one case, the perpetrator recommended a liquidity pool site, which “was a fraud site utilizing the brand of Allnodes, an established decentralized finance platform provider” (C33; Sophos, 2023a). When the victim purchased the ‘mining certificate’ that the offender suggested, the victim actually signed a smart contract that gave control of his wallet to the offender (i.e., when he bought the ‘mining certificate,’ he clicked on a prompt from his Coinbase wallet app that did not clearly explain he was signing over full access to his money). GASO (2021a) delineated how this was possible when they identified the Coinbase Wallet app flaw when communicating with perpetrators engaging in hybrid investment fraud and following their instructions:

While speaking with one of these ‘crypto mining’ scammers, I downloaded Coinbase Wallet and visited the scam site...With no money in my wallet, I pressed a button from within the Coinbase Wallet browser to join the mining pool, and just like that the scam website attempted to initialize the smart contract. Since I had no money in my wallet, I was informed that I didn’t have enough money to join the pool. However, if I did have the required funds, a smart contract would have been authorized by Coinbase Wallet without my informed consent, leading me into one of these never-ending subscriptions that could drain my wallet within a year, a month, or even a day. This clearly is a just cause for alarm...Coinbase must hand over an authentication key to the scam ... [app] in order to initiate the contract, yet makes no mention of this to the user, nor asks the user to affirm their consent to hand over this authentication key.

Thus, perpetrators of hybrid investment fraud not only take advantage of victims’ limited knowledge of trading processes by promoting fraudulent investments based on real investment processes, but also exploit vulnerabilities in existing platforms and apps to surreptitiously perpetrate the fraud.

Moreover, disinformation, misinformation, and conflicting information online complicated victim’s efforts to identify the fraud. Some fraudulent websites and/or fraudulent information provided by the offenders is easier to identify than others. For example, a fraudulent site identified in one of our cases (C39), Coinrule-web3, was covered by a website in a ‘news story’ identifying the platform as a preferred financial investment platform (Platte-Valley News Channel Nebraska, 2023). While there were instances of victims conducting research to determine if what was being presented was fraudulent, these

individuals were unable to accurately identify the fraud for various reasons. For instance, a victim conducted online research after being asked to pay taxes when attempting to withdraw invested cryptocurrencies (C25); when the victim came across information that stated that the Chinese government requires 20% on any transactions, the victim paid the ‘taxes.’

Further, offenders lied to conceal their true whereabouts and to explain inconsistencies in their actions and stories. When perpetrators were outside of the United States, such as those in Namibia, they operated during specific times to account for the time difference with the U.S. to make it seem as if the offenders were in the same or close to the same time zone as the victim (C20). Additionally, to explain contacting the victim from a different phone number, the offender claimed that his phone was hacked (C53).

Finally, the offender, who pretended to be the victim’s friend or in a romantic relationship, would feign having similar experiences with investment platforms, particularly when fees were required to withdraw funds. Specifically, in hybrid investment fraud, to obtain as much money as possible from victims, they are asked to pay fees, penalties, taxes and/or other charges when they attempt to withdraw investment funds. One victim in a case with multiple victims (C25), contacted an offender (the person who he fostered a relationship with) to discuss the fees the representative of the platform told him about. The offender substantiated the representative’s claim by falsely claiming that when her account was supposedly more than \$10,000,000 USD, she was informed that she had to pay \$1.8 million USD to unfreeze the account. The offender also falsely stated that she was able to unfreeze her account and access her funds after making the payment. Another offender who targeted a different victim in this case went so far as to provide a screenshot from the Chief Financial Officer of the (fraudulent) platform that would guarantee that the victim would be able to withdraw their funds if a final verification fee was paid. However, after paying this fee, the victim was asked to pay another \$50,000 USD for a blockchain congestion fee, and after paying that fee was asked for another \$100,000 USD to become a VIP member of the platform. Once this payment was made, the victim was notified that the withdrawal was successful but never received any funds and the offender and the platform could not be reached.

4.4.4.5. OPSEC measures. The offenders engaged in operational security (OPSEC) measures to make it more difficult to identify, investigate, and prosecute them. To make it harder to trace stolen cryptocurrency, offenders would transfer it to multiple “private wallets and swapping services” ([U.S. Attorney’s Office, Eastern District of Virginia, 2022](#)). In one case (C15), proceeds were commingled and deposited into numerous accounts. In another case with multiple victims, the stolen funds from one victim “were swapped from BTC to USDT using imToken and Tokenlon. The USDT was consolidated into wallet address and then rapidly transferred into and out of multiple intermediary wallet addresses, where they were commingled with other funds” (C25; [In the Matter of Application by the United States for Seizure Warrant, 2022](#)). This process is known as “chain hopping,” where “the holder of cryptocurrency converts it from one from [sic] of cryptocurrency to another—for instance, converting Bitcoin to Ethereum. When cryptocurrency is converted, it can make it harder to trace because it will often result in the currency being moved onto a separate blockchain ledger” (C4; [United States of America v. 5,012,294.90 in TetherUS et al., 2023](#), p. 28).

To protect their identities, our dataset revealed that offenders opened bank and cryptocurrency accounts using false names. For example, in [United States of America v. Jin Hua Zhang, et al. \(2022\)](#), forged Chinese passports and other individuals’ identification documents were used to conceal offenders’ identities (C17). To cover their tracks, offenders have also instructed victims to delete messages between them (C2); to conceal the reason for wire transfers by writing ‘other’ in the reasons for the transfer (C3) or sending the wires to

companies with names (e.g., HomeGoods LLC; C54) that would not be flagged as suspicious and would avoid drawing the attention of authorities; and to delete their social media account because it was not ‘safe’ (C25). Offenders have also added false reasons for the receipt of funds and/or have created fake invoices to justify the receipt of funds from victims, such as claiming that payment was received for the sale of toys, electronics, or other goods (e.g., C54), among other reasons.

4.4.5. *The fraud reveal*

If the target cannot pay and/or refuses to provide any more funds, communications between offender, target, and others involved in the fraud cease (with few exceptions). Overall, the target does not recover some or all the funds (with few exceptions identified in the literature; see ([Farivar, 2023](#)). Our dataset revealed that the fraud was identified in a variety of ways. This stage is like [GASO’s \(n.d.\)](#) “killed” stage and [FinCEN’s \(2023\)](#) “point of no return” stage.

4.4.5.1. *Conducted research.* In certain cases, the fraud was identified after victims engaged in research. For example, one victim discovered the fraud after contacting Sophos (a cybersecurity company) and reviewing an article published by them on liquidity mining (C33). The victim was informed that he was a victim of fraud and was told to block and cease communications with the perpetrators. Other victims conducted research after either experiencing a negative consequence (e.g., being unable to withdraw money and/or being told money was needed to make withdrawal) or after an organization or agency informed them of potential fraudulent transactions. After being told by a customer service representative of the platform he was using to provide \$1.5 million USD to withdraw his money, a victim searched online and found a U.S. Federal Bureau of Investigation (FBI) alert for this fraud (C51).

4.4.5.2. *Family members, friends, and coworkers.* Several of the victims in our dataset were alerted to the fraud by friends and families. For example, in one case (C25), a victim realized it was a fraud when he sought a home equity loan to pay taxes and his family questioned his investment. In another case (C26), a friend informed a victim of hybrid investment fraud after the victim shared information about her relationship with the offender (C26). Coworkers questioned another victim when she liquidated her 401k (C28).

Further, in one case, the fraud was revealed by a husband who formed a remote romantic relationship with a woman who encouraged him to leave his wife during their ‘relationship’ (C39). The woman convinced him to liquidate his joint investments with his wife to invest more than \$9 million USD in cryptocurrency investments ([Krasilnikova, 2023](#)). This fraud was revealed when the husband contacted his wife to liquidate the remaining assets to pay the requested ‘fee’ needed to withdraw his profits.

4.4.5.3. *Government agencies and banks.* A few victims realized they were the target of fraud when they contacted government authorities. For instance, in one case with multiple victims (C25), when one victim sought to withdraw money from their account, he was informed by the platform that taxes needed to be paid according to the IRS Blockchain Technology Cryptocurrency Authority. The victim contacted the US Internal Revenue Service and asked about the IRS Blockchain Technology Cryptocurrency Authority but was informed that no such agency exists. Nonetheless, our dataset did not reveal that taxes were questioned by all victims. In one case (C6), a purported customer service agent informed the victim that before a withdrawal is made a 25% tax must be paid to the International Tax Bureau (a bureau that does not exist). In another case, a bank manager informed a victim of the fraudulent scheme when the victim went to the bank to wire money to an account the offender provided (C54).

4.4.5.4. *Cryptocurrency exchanges.* Certain victims in our dataset identified the fraud after reporting issues with withdrawing their funds to cryptocurrency exchanges and/or regulatory agencies. For

instance, one victim learned of the fraud when the victim reported being unable to withdraw funds to Coinbase and Bitstamp. Crypto.com reached out to one victim to inform them of unusual transactions linked to frauds. Particularly, Crypto.com flagged some of the victim's transactions as being linked to wallet addresses associated with fraud and asked the victim to review the transactions (C8). Following this notification, the victim conducted online research and found a fraud alert by the California Department of Financial Protection and Innovation for the platform the victim was using.

4.4.5.5. Customer service issues and multiple fees requested for withdrawals of funds. Some victims identified the fraud because of the various excuses given as to why payment of funds could not be made as well as the new fees that were requested for withdrawals each time a fee was paid, and a request was made for payment. One victim was asked to pay a "risk deposit" fee after requesting to withdraw a portion of his funds. Once this was paid, he attempted to withdraw the money, only to be asked to pay another fee. Following this new request for money, he realized he was a victim of fraud (C54). Another victim realized that she was a victim of fraud when she was informed that she could not withdraw her money without paying taxes, which could not be deducted from the gains in her account (C14).

4.4.5.6. Offenders stop communicating with the victims and/or the fraudulent app or website disappears. In most of our cases, when offenders receive a substantial sum, the target sum, and/or the victim can no longer pay and/or no longer wants to pay fees and is requesting their funds, the offenders and associates (in the form of customer service and other representatives of the fraudulent platforms) eventually "ghost" the victims by becoming non-responsive and abruptly ceasing communications. After paying several fees when attempting to withdraw funds and being unsuccessful each time, the representative of the fraudulent platform becomes unreachable. In such cases, the listed fees and the payment amount that is reached before communications between representatives of the fraudulent platform and the victim cease varied by case. For instance, after wire transferring fee money to the offender, the offender immediately stopped communicating with the victim and the fraudulent site disappeared (C54). In most of the cases in our dataset, the offender(s) that initiated contact with the victim and fostered a relationship with the victim also became unreachable around the same time. In only one case did we identify a perpetrator who "revel[ed] in unveiling the financial — and emotional — deception" to the victim (C36; Podkul, 2022).

4.4.6. Important outliers and deviations from known offender patterns

4.4.6.1. Video calling as a confidence building measure. Our dataset included cases where the offenders agreed to engage in a video call with the victims.

The public is often warned to be wary of individuals who they meet online who refuse to either meet in person and/or engage in video calls (FINRA, 2022). While we only identified a few cases in our dataset where offenders' video called victims, this is an important finding as victims identified this action as a confidence building measure in the relationship and investments. Video chats were also used to share information to build victims' confidence in the investment. For example, in one case (C54), the offender showed the victim statements to substantiate her claims of millions in earnings in a video call. Nevertheless, we also identified cases in our dataset where perpetrators refused video calls and in person meetings for different reasons.

4.4.6.2. More than one offender targeted the same victim. A few cases in our dataset revealed that the same victim was targeted by more than one offender, who may or may not have been working together (from available information, this connection could not be established). For example, in one case (C2), the victim was contacted by the perpetrator (claiming to be Hao William Yang), who was interested in viewing the

victim's San Francisco home. When the victim similarly received multiple messages from other Asian men asking to see the San Francisco property, the victim told the perpetrator about this odd occurrence. The perpetrator responded angrily and accused the victim of cheating to divert attention away from this incident.

In the other case (C32), the offender (who used the persona of a Chinese woman named 'Hui Hui') reached out to the victim via social media. While the chat began friendly, it then turned romantic. While communicating with Hui Hui and investing \$18,000 USD of his funds, the victim was also contacted by another Chinese woman named 'Lydia' on social media and formed a friendship. The victim expressed suspicions to Lydia about the money he invested with Hui Hui. Lydia informed him of another cryptocurrency investment opportunity after three months of communicating. He invested \$20,000 USD into the second investment opportunity. After learning he could easily withdraw money from the second investment platform, he decided to invest more money. When he attempted to withdraw his money from the first platform, he was told he had to pay a \$132,000 USD penalty. Following his failed attempt to withdraw funds from the first investment platform, he tried to withdraw funds from the second platform. The second platform also informed him that he must pay a \$50,000 USD penalty. After these failed attempts, he realized he was a victim of fraud by both offenders.

In the third case (C25), in March 2022, the victim was contacted by someone named 'Eden Lin' on LinkedIn and developed a friendship. While the victim was sick with COVID-19, the offender introduced her to future trading and encouraged her to invest her cryptocurrency, money from her bank account, and money from liquidated retirement accounts to mcus.me. When attempting to withdraw funds from her investment, she was informed her account was frozen and a deposit of \$293,000 USD was needed to reactivate her account. After notifying the offender that she was only able to raise \$80,000 USD, she was instructed to wire transfer those funds to him. After sending the wire transfer, the mcus.us site was no longer accessible, and the offender stopped responding to her communications. In May 2022, the same victim was engaged by someone named 'Zelin Wang,' who purportedly needed advice with launching a company. After forming a friendship, the offender introduced the victim to Top Tank, where she invested \$40,000 USD. When she attempted to withdraw funds, her account was "frozen" and she was informed she had to pay \$60,000 USD to unfreeze her account and withdraw her money. The victim was unable to recover funds from either site. Likewise, another victim was targeted in two separate incidents by offenders identifying as women ("Unity/Sakurako" and "Emma/Annie Catherine") (C16).

Barring further details in these cases to show connections between perpetrators, the second hybrid investment fraud attempt could be alternatively interpreted as instances of what Button and Cross (Button and Cross, 2017) termed as recovery fraud, where victims experience revictimization.

4.4.6.3. Private and financial information. One victim provided personal information to open an account, and after he was denied, he was told he would need to submit a copy of his driver's license and passport (C55). Other victims were told to upload driver's licenses to platforms for verification reasons (C21), asked to provide driver's license and bank information (C25), and bank statements and "confidential, personally identifying information" (C9). The provision of this information exposes the victims to further forms of fraud, including identity theft and other forms of fraud. Government consumer protection alerts include warnings to victims to avoid sharing personal and financial information with strangers and online apps, platforms, and/or sites that cannot be authenticated (e.g., State of Michigan Attorney General, n.d.; FTC, n.d.; Federal Deposit Insurance Corporation FDIC, 2021; U.S. Department of Justice, 2023).

4.4.6.4. Money requested for emergency. In one case in our dataset (C45), which involved various frauds perpetrated by the offender, one of which was a specific form of hybrid investment fraud - romance

baiting, the offender sought money from one victim for an emergency. This finding conflicts with the understanding that the “request for money is not attributed to an emergency” in romance baiting (Cross, 2023, p. 5). The fraud in the case began as a traditional romance fraud, and then turned into a cryptocurrency investment fraud. The sequence of events of the fraud were as follows:

- the victim and offender developed a purely online relationship;
- the offender asks for assistance in purchasing medical equipment with the understanding that the victim would be reimbursed;
- the victim sends the money;
- the offender claims to be injured and in need of money for medical bills;
- the victim sends the money;
- documents are used to support the offender’s claims and a ‘third party’⁷ reaches out to make stories of the offender more believable to obtain even more money from the victim (i.e., pretended to be a doctor, sent a purported photo of the victim on a hospital bed, and requested money for the victim);
- the offender states that she will reimburse the victim and provides an excuse as to why this reimbursement is not possible (i.e., the victim’s bank would not accept the money);
- the offender offers to invest the victim’s money in a cryptocurrency investment platform known as Alphacoin Lab so the victim could obtain the funds;
- the offender sets up an account for the victim on this platform;
- several representatives of this cryptocurrency exchange email the victim and message the victim via WhatsApp;
- the victim is informed that he could withdraw the funds after paying taxes and fees on the funds via wire transfer; and
- the victim wire transfers the taxes and fees.

Ultimately, after paying taxes and fees, the victim was unable to withdraw the funds.

4.4.6.5. NFTs. The limited literature on hybrid investment fraud predominantly focuses on cryptocurrency investments, and to a lesser extent gold. While our research likewise predominantly identified frauds involving the cryptocurrency trade, and to a lesser extent gold, we also identified a case that involved the trade of non-fungible tokens (NFTs). Specifically, our dataset included one case where a victim was conned into investing in NFTs via a fraudulent trade website (C54).

4.4.6.6. Artificial intelligence and ChatGPT. One case in our dataset involved a victim who contacted Sophos to report a hybrid investment fraud that involved the use of an artificial intelligence (AI) based tool, like ChatGPT (C38). The victim connected with the offender when using Tandem, a language app that has been used as a dating app. After the communications between victim and offender moved to WhatsApp, “[t]he victim became suspicious after he received a lengthy message that was clearly partly written by an AI chat tool using a large language model (LLM)” (C38; Pawaon, 2023). The use of pre-written scripts for hybrid investment fraud is consistent with the findings of Wang and Zhou (2023).

4.4.7. Responses to hybrid investment fraud

The cases in our dataset revealed that U.S. authorities have taken several measures to respond to hybrid investment fraud, including civil forfeiture and other civil actions against offenders and companies; seizing spoofed domains; administrative cease and desist orders; seizing financial accounts and cryptocurrency wallets; and arresting offenders. For the offenders criminally charged, the most common charges

included wire fraud, bank fraud, money laundering, unlicensed money transmitting business, conspiracy to commit wire fraud, bank fraud conspiracy, and conspiracy to commit money laundering.

5. Limitations

A main limitation of our study is the number of identified hybrid investment fraud cases. We encountered significant difficulties in identifying these cases. The colloquial term of ‘pig butchering’ was not always used. Also, various terms were used in cases and news articles to describe hybrid investment fraud, including romance baiting, cryptorom scams, cryptocurrency investment scheme, cryptocurrency scams, crypto catfishing, cryptocurrency confidence schemes, and cryptocurrency confidence scams. The inconsistent terms used to describe hybrid investment fraud made the identification of these cases extremely difficult. What is more, many of these terms are limiting, and exclude other cases of hybrid investment fraud. Specifically, the limitation of these terms to romance and cryptocurrencies omits cases where other forms of relationships were sought and other forms of investments. Furthermore, cases were difficult to identify as information about hybrid investment fraud was scattered over various news articles and administrative, civil and/or criminal court documents.

Our sample is not a representative sample of all hybrid investment fraud cases in the United States. Our sample also could not draw on existing crime measurement tools as they do not report hybrid investment fraud. For this reason, we reiterate the sentiment expressed in Lazarus et al.’s (2023) systematic review that more diverse data is needed and extend this perspective to news coverage, arguing that more diverse cases from a wider regional and global range must appear in the news along with more rich empirical data to fully understand the nature and extent of hybrid investment fraud. We followed a similar exploratory approach, the analysis of court documents and news articles, which has been used to study other forms of crime (e.g., Arsovská and Temple, 2016; Button and Cross, 2017; Maras and Arsovská, 2023). The content in private legal databases is constantly updated. The number of cases we identified were dependent on the dates in which we conducted the search, our search process, the terms we used, the process we used to exclude cases from our dataset, the information available in the documents, and the time period of the search.⁸ By triangulating our sources, we were able to identify the elements of hybrid investment fraud, victims of this fraud, and the tactics, tools, targets, and methods of operation of offenders. Our exploratory research covered an understudied topic and filled an important gap in academic literature.

6. Conclusion

Our research revealed that existing fraud typologies, which were designed to clarify differences between various forms of fraud and serve as a comprehensive inventory of all types of fraud, do not adequately address the evolution of fraud, particularly hybrid fraud. Hybrid fraud, like hybrid investment fraud, combines tactics, tools, and methods of operation from different forms of fraud. Perpetrators of this fraud take operational security measures to evade detection, investigation, and prosecution, and engage in tactics to obscure the fraud. Hybrid fraud is a complex phenomenon with devastating psychological, social, and financial impacts.

Our research revealed offenders prey on people’s desire for companionship and seek to gain victims’ confidence and trust by creating an illusion of credibility and success, using images of attractive people,

⁷ This may not actually be a third party. It can be the offender pretending to be another party.

⁸ For example, even when two researchers conducted the search separately on the same day at the same time using the same criteria on LexisNexis, the number of results returned varied (after clearing cache and running the same search in the same order, our search returned the same results).

promoting extravagant lifestyles, and claiming expertise in trading and investment knowledge to lure people first into fake connections and/or relationships and then fraudulent investment schemes. While many cases did involve the fostering of romantic relationships between victims and offenders and investments in cryptocurrencies, there were cases where relationships were not romantic in nature (i.e., friendship) and involved investments in gold and NFTs. The offenders used persuasive language, a sense of urgency, and confidence building and coercive measures to pressure victims to invest and provide additional funds to their original investments. The tactics used are designed to 'drain' victims of their funds to obtain as much money from them as possible, often recommending that the victims obtain loans, liquidate savings and retirement funds, and reach out to family and friends for financial assistance.

We use the term hybrid investment fraud to describe what is colloquially known as pig butchering, as the colloquial term dehumanizes victims and their experiences and does not adequately capture the multifaceted nature and the ultimate goal of this fraud. Our research advanced knowledge in the field by shedding light on the understudied topic of hybrid investment fraud. With our work, we hope to inspire the use of similar terms to describe the same phenomena in the literature, news, and cases, particularly the use of the word 'hybrid' to describe forms of cyber-enabled fraud that combine tactics, targets, tools, and elements of the methods of operation of perpetrators of different types of fraud. Moreover, we aim to stimulate future research on this topic and encourage the modification of existing fraud typologies to capture hybrid fraud.

CRediT authorship contribution statement

Marie-Helen Maras: Writing – review & editing, Writing – original draft, Supervision, Resources, Project administration, Methodology, Investigation, Formal analysis, Conceptualization. **Emily R. Ives:** Writing – review & editing, Resources, Methodology, Investigation, Formal analysis.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

- Albert Abed, v Wei Lin, Melis, Case 1:23-cv-21059, Plaintiff's Memorandum of Law in Support of his Motion for a Preliminary Injunction (U.S. District Court for the District of New Jersey, October 11, 2023).
- Access Wire, 2022. The Slaughtered Love: RealCall's Survey Finds 96.08% of Americans Were Targeted by Pig Butchering Scams. December 1, 2022. <https://www.accesswire.com/729424/The-Slaughtered-Love-RealCalls-Survey-Finds-9608-of-Americans-Were-Targeted-by-Pig-Butchering-Scams#:~:text=555%2D555%2D555,The%20Slaughtered%20Love%3A%20RealCall's%20Survey%20Finds%2096.08%25%20of%20Americans%20Were,Targeted%20by%20Pig%20Butchering%20Scams&text=A%20new%20survey%20conducted%20by%20expanded%20and%20caused%20huge%20losses.> (Accessed 28 December 2023).
- Adebayo, O., 2023. US authorities crackdown on pig butchering crypto scams. Newstex Blogs (NexisUni database). Cryptopolitan, September 28, 2023. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:698M-CYK1-JCMN-Y108-00000-00&context=1516831>. (Accessed 13 February 2024).
- Alabama Securities Commission, 2022. Alabama Investor Loses Over \$40,000 in Pig Butchering Scam. https://asc.alabama.gov/wp-content/uploads/2023/11/13-24-2022_Pig_Butchering_Scam.pdf (Accessed 13 February 2024).
- Allen, F., 2021. Porky Pies - I lost £60k in new 'pig butchery' crypto scam when dating site fraudster brainwashed me into investing in fake scheme (NexisUni database). Sun (November 3, 2021. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:6408-82B1-DY4H-K3VP-00000-00&context=1516831>.
- Anuforo, C., 2023. Scammers add ChatGPT to their toolset – Sophos report (NexisUni database). Sun (<https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:68WH-J041-JDJN-6376-00000-00&context=1516831>) (Accessed 13 February 2024).
- Armstrong, T., 2023. Dad reveals he lost half a million dollars, his home and WIFE after falling victim to cruel 'pig butchering' scam - as figures show Americans are losing record amounts to crypto fraudster (NexisUni database). MailOnline, July 31, 2023. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:68W2-Y971-DY4H-K081-00000-00&context=1516831> (Accessed 13 February 2024).
- Arsovka, J., Temple, M., 2016. Organizational learning, adaptation, and rationality: The expansion of Albanian organized crime in New York City. *Crime, Law and Social Change* 66 (1), 1–20.
- Australian Competition and Consumer Commission, 2023. Targeting scams: report of the ACCC on scams activity 2022. <https://www.accc.gov.au/about-us/publications/serial-publications/targeting-scams-report-on-scams-activity/targeting-scams-report-of-the-accc-on-scams-activity-2022>. (Accessed 5 May 2023).
- Bartlett, S., 2023. Woman says she was victim of 'pig butchering' dating scam - and lost £360k. (NexisUni database). *The Daily Star* https://www.dailystar.co.uk/love-sex/woman-says-victim-pig-butchering-30024018?utm_source=mynewsassistant.com&utm_medium=referral&utm_campaign=embedded_search_item_desktop [provided on NexisUni by Daily Star].
- Beals, M., DeLiema, M., Deevy, M., 2015. Framework for a Taxonomy of Fraud. *Stanf. Cent. Longev.* 1–40.
- Bilz, A., Shepherd, L.A., Johnson, G.I., 2023. Tainted love: a systematic literature review of online romance scam research. *Interact. Comput.* <https://doi.org/10.1093/iwc/iwad048>
- Brian Hoop v. Emma Doe and John Does I-XX, and 177.7621 ETHER, and MEXC GLOBAL, LLC. Compliant Case 4:23-cv-00185-SMR-HCA (U.S. District Court for the Southern District of Iowa Central Division, June 5, 2023).
- Buchanan, T., Whitty, M.T., 2013. The online dating romance scam: Causes and consequences of victimhood. *Psychol. Crime. Law* 20 (3), 261–283. <https://doi.org/10.1080/1068316X.2013.772180>
- Button, M., Cross, C., 2017. Cyber frauds, scams and their victims. Routledge. <https://doi.org/10.4324/9781315679877>
- Carter, E., 2020. Distort, extort, deceive and exploit: exploring the inner workings of a romance fraud. *Br. J. Criminol.* 61 (2), 283–302. <https://doi.org/10.1093/bjc/azaa072>
- CE Noticias Financieras English, 2022a. Dating apps, the new target of crypto-scammers: how to protect yourself from crime (NexisUni database). 23 February 2022. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:64VN-VNW1-DYY9-00T1-00000-00&context=1516831>.
- CE Noticias Financieras English, 2022b. How a woman lost US\$ 2.5 million with a WhatsApp message (NexisUni database). 13 April 2022. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:6574-7TC1-DYY9-01DW-00000-00&context=1516831> (Accessed 13 February 2024).
- Chandriaiah, J., Wu, X., 2021. CryptoRom fake iOS cryptocurrency apps hit US, European victims for at least \$1.4 million. Sophos, October 13, 2021. <https://news.sophos.com/en-us/2021/10/13/cryptorom-fake-ios-cryptocurrency-apps/> (accessed 5 May 2023).
- China News, 2019. Top 10 new words in Chinese media in 2019, including night economy, extreme pressure and more. <https://www.chinanews.com.cn/gn/2019/12-16/9034981.shtml>. (Accessed 5 November 2023).
- Citron, D.K., 2014. Hate Crimes in Cyberspace. Harvard University Press. <https://doi.org/10.4159/harvard.9780674735613.c13>
- Coluccia, A., Pozza, A., Feretti, F., Carabellese, F., Masti, A., Gualtieri, G., 2020. Online romance scams: Relational dynamics and psychological characteristics of the victims and scammer. A scoping review. *Clin. Pract. Epidemiol. Ment. Health* 16 (1), 24–35. <https://doi.org/10.2174/174501790201601002>
- Commodity Futures Trading Commission, v. Cunwen Zhu and Justby International Auctions, Case 2:23-cv-04937, Complaint for Injunctive and Other Equitable Relief and for Civil Monetary Penalties Under the Commodity Exchange Act and Commission Regulations (U.S. District Court for the Central District of California, June 22, 2023).
- Cross, C., 2019. "You're not alone": the use of peer support groups for fraud victims. *J. Hum. Behav. Soc. Environ.* 29, 672–691. <https://doi.org/10.1080/10911359.2019.1590279>
- Cross, C., 2023. Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud. *Curr. Issues Crim. Justice* 1–13. <https://doi.org/10.1080/10345329.2023.2248670>
- Cross, S., Hirrelle, S., Lim, M.-A., 2021. *Cybercrime Strategy Guidebook*. Interpol.
- Cross, C., Holt, T., 2021. The use of military profiles in romance fraud schemes. *Vict. Offenders* 16 (3), 385–406. <https://doi.org/10.1080/15564886.2020.1850582>
- Cross, C., Holt, K., O'Malley, R., 2022. If u don't pay they will share the pics?: Exploring sextortion in the context of romance fraud. *Victims & Offenders* 18 (7), 1194–1215. <https://doi.org/10.1080/15564886.2022.2075064>
- Crypto Breaking News, 2023a. Report: Namibian Police Arrest 20 Ringleaders of Local Pig Butchering Crypto Scam (NexisUni database). 18 October 2023. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:69D-WTM31-JCMN-Y21C-00000-00&context=1516831> (Accessed 13 February 2024).
- Crypto Breaking News, 2023b. U.S. Justice Department Seizes Cryptocurrency Worth \$112 Million in 'Pig Butchering' Crackdown (NexisUni database). April 5, 2023. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:67 YO-WK61-F03R-N24W-00000-00&context=1516831> (Accessed 13 February 2024).
- Divya Gadasalli, an individual, v. Jerry Bulasa, an individual; Dong Lian, an individual; Danyun Lin, an individual; TD Bank, n.a., a National Banking Association; Abacus Federal Savings Bank, a Federal Savings Bank; Binance Holdings, LTD, d/b/a Binance, a Foreign Company; and Poloniex,LLC, a Delaware Limited Liability Company, Case 4:22-cv-00249-alm, Declaration of David C. Silver (U.S. District Court Eastern District of Texas, March 29, 2022).
- Drew, J.M., Webster, J., 2024. The victimology of online fraud: A focus on romance fraud victimisation. *J. Econ. Criminol.* 100053. <https://doi.org/10.1016/j.jecon.2024.100053>

- Ducklin, P. 2021. Romance scams with a cryptocurrency twist—new research from SophosLabs. <https://nakedsecurity.sophos.com/2021/10/13/romance-scams-with-a-cryptocurrency-twist-new-research-from-sophoslabs/> (Accessed 5 May 2023).
- Falcon, R., 2022. Dating apps, the new target of crypto-scammers: how to protect yourself from crime, Wate 6 (ABC), February 23, 2022. [https://www.wate.com/news/tennessee/woman-loses-390k-in-crypto-from-hinge-romance-scammer/#:~:text=\(NEXSTAR\)%20E2%80%94%20A%204%2D,cryptocurrencies%20to%20hide%20their%20identities](https://www.wate.com/news/tennessee/woman-loses-390k-in-crypto-from-hinge-romance-scammer/#:~:text=(NEXSTAR)%20E2%80%94%20A%204%2D,cryptocurrencies%20to%20hide%20their%20identities) (Accessed 13 February 2024).
- Farivar, C., 2022. ‘Pig Butchering’ Crypto Scam Victim to Get Money Back from Binance, Law Enforcement Says. Forbes, July 1, 2022. <https://www.forbes.com/sites/cyrusfarivar/2022/07/01/pig-butchering-crypto-scam-victim-to-get-money-back-from-binance-law-enforcement-says/?sh=3819d6745ecd> (Accessed 5 November 2023).
- Farivar, C., 2023. They Lost Millions to Crypto Scammers. This Prosecutor Is Helping Them Get It Back. Forbes, January 17, 2023. https://countyda.sccgov.org/sites/g/files/exjcpb1121/files/documents/They%20Lost%20Millions%20To%20Crypto%20Scammers.%20This%20Prosecutor%20Is%20Helping%20Them%20Get%20It%20Back_.pdf (Accessed 5 November 2023).
- Faux, Z., 2023. ‘Don’t you remember me?’ The crypto hell on the other side of a spam text. The Business Standard, August 18, 2023. <https://www.ibsnews.net/bloomberg-special/dont-you-remember-me-crypto-hell-other-side-spam-text-684258> (Accessed 5 November 2023).
- Federal Bureau of Investigation (FBI) and Internet Crime and Complaint Center (IC3), 2023. The FBI Warns of False Job Advertisements Linked to Labor Trafficking at Scam Compounds. Alert Number I-052223-PSA. <https://www.ic3.gov/Media/Y2023/PSA230522> (Accessed 5 November 2023).
- Federal Deposit Insurance Corporation (FDIC), 2021. Avoiding Scams and Scammers. <https://www.fdic.gov/resources/consumers/consumer-news/2021-10.html> (Accessed 28 December 2023).
- Federal Trade Commission (FTC), 2021. FTC Online Complaints (Filed: October 14, 2021). <https://ecid.documentcloud.org/documents/22418617/ftc-pig-butchering-scam-complaint.pdf> (Accessed 13 February 2024).
- Federal Trade Commission (FTC), n.d. Heads up: Stop. Think. Connect. <https://consumer.ftc.gov/articles/heads-up> (Accessed 28 December 2023).
- FinCEN, 2023. FinCEN Alert on Prevalent Virtual Currency Investment Scam. Commonly Known as “Pig Butchering.” FIN-2023-Alert005 https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf (Accessed 5 November 2023).
- FinCEN, 2022. FinCEN Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering.” FinCEN Alert, FIN-2023-Alert005. https://www.fincen.gov/sites/default/files/shared/FinCEN_Alert_Pig_Butchering_FINAL_508c.pdf (Accessed 5 November 2023).
- FINRA, 2022. ‘Pig Butchering’ Scams: What They Are and How to Avoid Them. <https://www.finra.org/investors/insights/pig-butchering-scams>. (Accessed 5 November 2023).
- FINRA, 2024. Be Alert to Signs of Imposter Investment Scams, <https://www.finra.org/investors/insights/be-alert-signs-impostor-investment-scams> (Accessed 16 March 2024).
- Fletcher, E., Consumer Protection Data Spotlight, 2023. Social media: a golden goose for scammers. Federal Trade Commission (FTC), <https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers> (Accessed 5 November 2023).
- GASO, 2021a. Coinbase Wallet Has a Major Security Vulnerability. <https://www.globalantiscam.org/post/coinbase-s-lack-of-accountability-presents-a-security-vulnerability> (Accessed 28 December 2023).
- GASO, 2021b. Dating apps and social media tech: responsible and irresponsible? <https://www.globalantiscam.org/post/dating-apps-and-social-media-tech-responsible-and-irresponsible>. (Accessed 28 December 2023).
- GASO, 2021c. Fake Investors Group Chat <https://www.globalantiscam.org/post/fake-investors-group-chat> (Accessed 16 March 2024).
- GASO, n.d. The Pig Butchering Scam. <https://www.globalantiscam.org/about>.
- GASO, 2022. Statistics of crypto-romance/pig-butchering scam. <https://www.globalantiscam.org/post/statistics-of-crypto-romance-pig-butchering-scam> (Accessed 28 December 2023).
- Goode, L., 2023. Dating Apps Crack Down on Romance Scammers. Wired, February 14, 2023. <https://www.wired.com/story/dating-apps-tools-to-thwart-scams/> (Accessed 5 November 2023).
- Gordon, S., Ford, R., 2006. On the definition and classification of cybercrime. J. Comput. Virol. 2, 13–20. <https://doi.org/10.1007/s11416-006-0015-z>
- Governance, Risk & Compliance Monitor Worldwide, NJ attorney general announces crackdown on ‘pig butchering’ schemes (LexisNexis database). 7 February 2023. <https://advance.lexis.com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:67GW-NHD1-F11P-X3NX-00000-00&context=1516831> (Accessed 13 February 2024).
- Governance, Risk & Compliance Monitor Worldwide, 2022. Cryptocurrency broker RB Hood appears to be engaged in fraud against California consumers (LexisNexis database). 29 December 2022. <https://advance.lexis.com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:676B-V5N1-JDJDN-6231-00000-00&context=1516831> (Accessed 13 February 2024).
- Garung, Anjita v. Metaquotes LTD, a Cyprus Corporation; Metaquotes Software corp., a Bahamas Corporation; Metaquotes Software Corp., a Delaware Corporation; Forexware LLC, a delaware limited liability company; sich capital LTD, a United Kingdom Corporation; OPSO, Case 1:23-cv-06362-oem-pk, Plaintiff's Omnibus Opposition to Defendants' Motions to Dismiss the Complaint (United States District Court Eastern District of New York, 2023).
- Ibrahim, S., 2016. Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. Int. J. Law Crime. Justice 47, 44–57. <https://doi.org/10.1016/j.ijlcj.2016.07.002>.
- ICE, 2021. 2021 Internet Crime Report. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf. (Accessed 5 November 2023).
- In Re Bien, Case 3:22mc80191, Amended Motion to Amend/Correct ex parte Application Filed by Rachel Bien, (U.S. District Court for the Northern District of California, October 27, 2022).
- In the Matter of Application by the United States for Seizure Warrant for the Accounts for Investigation of 18 U.S.C. Section 1343 and other offenses, Case 3:22-mj-71553-AGT, Application for a Warrant to Seize Property Subject to Forfeiture (U.S. Northern District of California, November 30, 2022).
- In the matter of Cresttrademining Limited, Summary Cease and Desist order (State of New Jersey, Bureau of Securities, 2023).
- In the matter of Forex Market Trade, Summary Cease and Desist order (State of New Jersey, Bureau of Securities, 2023).
- In the matter of MetaCapitals Limited, Summary Cease and Desist order (State of New Jersey, Bureau of Securities, 2023).
- In the Matter of Seizure of any and all funds and/or other negotiable instruments stored in the account held by Binance associated with User Identification number redacted held in the name of redacted. Case 2:22 MJ-04906, Application and Affidavit for Seizure Warrant (U.S. District Court of California, December 15, 2022).
- In the Matter of the Seizure of Funds not to Exceed \$351,000.00 in Wallets at Binance Holdings Limited as Described in the June 6, 2022, Affidavit of TFO James Jackson, Case 2:22-cr-00608-mgb, Application for a Warrant to Seize Property Subject to Forfeiture (U.S. District Court for the District of South Carolina, June 07, 2022).
- In the Matter of the seizure of the domain names simexcrb.com, simexlu.com, simexwim.com, simexarts.com, simexrue.com, simexvtm.com and simexbiz.com, Case 1:22-sw-00596-WEF (U.S. Eastern District of Virginia, November 16, 2022).
- In the matter of up to 489,269.52 Tether (usdt) Cryptocurrency on case number: deposit in the kraken user id aa27 n84g rdv7 whda held in the name of osl sg pte ltd, Case 23 mj 160, Application for a Warrant (Eastern District of Wisconsin, September 11, 2023).
- In the matter of www.batcipe.vip, James Yeh, www.batcnap.vip, Kenju Go, Administrator Order No. CD-2023-0011 (Alabama Securities Commission, July 6, 2023).
- Internet Crime Complaint Center (IC3), 2021. Internet Crime Report 2021. U.S. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (Accessed 5 November 2023).
- Internet Crime Complaint Center (IC3), 2022. Internet Crime Report 2022. U.S. Federal Bureau of Investigation. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf (Accessed 5 November 2023).
- Jane, E.A., 2016. Online misogyny and feminist vigilantism. Continuum 30 (3), 284–297. <https://doi.org/10.1080/10304312.2016.1166560>
- Keaton, J., 2023. UN Warns that Hundreds of Thousands in Southeast Asia have been Roped Into Online Scams. Associate Press. <https://apnews.com/article/cambodia-myanmar-migrants-online-scams-ebab962f236df69b1f9b7e136958e244> (Accessed 5 November 2023).
- Kelly, H., 2023. Newly-divorced mum reveals how she lost \$100,000 to man she met on Tinder in ‘pig butchering’ scam – here’s the red flags she ignored (NexisUni database). MailOnline {C}18(C), June 2023. <https://advance.lexis.com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:68GW-W511-DY4H-K2HD-00000-00&context=1516831> <https://www.dailymail.co.uk/news/article-12208425/Mum-reveals-lost-100k-man-met-Tinder-cruel-pig-butchering-scam.html> (Accessed 13 February 2023).
- Krasilnikova, O., 2023. Minnesota Resident Got Ripped Off \$9M In a Crypto Romance Scam. Cryptodaily, August 2, 2023. <https://cryptodaily.co.uk/2023/08/minnesota-resident-got-ripped-off-9m-in-a-crypto-romance-scam#:~:text=Minnesota%20police%20reported%20that%20the,losing%20%249million%20in%20total>. (Accessed 5 November 2023).
- Lazarus, S., 2019. Just Married: The Synergy between Feminist Criminology and The Tripartite Cybercrime Framework. Int. Soc. Sci. J. 69 (231), 15–33. <https://doi.org/10.1111/issj.12201>
- Lazarus, S., Button, M., Kapend, R., 2022. Exploring the Value of Feminist Theory in Understanding Digital Crimes. Howard J. Crime. Justice 61 (3), 381–398. <https://doi.org/10.1111/hojo.12485>
- Lazarus, S., Okolorie, G.U., 2019. The bifurcation of the Nigerian cybercriminals: Narratives of the Economic and Financial Crimes Commission (EFCC) agents. Telemat. Inform. 40, 14–26. <https://doi.org/10.1016/j.tele.2019.04.009>
- Lazarus, S., Whittaker, J.M., McGuire, M.R., Platt, L., 2023. What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). J. Econ. Criminol., 100013. <https://doi.org/10.1016/j.jecon.2023.100013>
- Lee, J., 2022. Pig butchering: A day in the life of a cyberfraud fighter (LexisNexis database). VentureBeat, 28 October 2022. <https://advance.lexis.com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:66R9-J1X1-JCMN-Y116-00000-00&context=1516831> (Accessed 13 February 2023).
- Leonard Tether Licht v. Tina Ling and Luxkey, Case 3:23-cv-01018-x, Plaintiff's Original Complaint (U.S. District Court for the Northern District of Texas Dallas Division, May 8, 2023).
- Levine, T.R., Kim, R.K., Hamel, L.M., 2010. People lie for a reason: An experimental test of the principle of veracity. Commun. Res. Rep. 27 (4), 271–285. <https://doi.org/10.1080/08824096.2010.496334>
- Lim, J., 2022. Stop Scams podcast: How an American business owner lost \$275k in a cryptocurrency scam. Straits (November 18, 2022. <https://www.straitstimes.com/singapore/courts-crime/stop-scams-podcast-how-an-american-business-owner-lost-275k-in-a-cryptocurrency-scam#:~:text=Home%20Stop%20Scams%20podcast%3A%20How%20an%20American%20business%20owner%20lost,k%20in%20a%20cryptocurrency%20scam&text=SINGAPORE%20E2%80%99%20Scams%20podcast%3A%20How%20an%20American%20business%20owner%20lost,k%20in%20a%20cryptocurrency%20scam> (Accessed 5 November 2023).
- Maras, M.-H., 2017. *Cybercriminology*. Oxford University Press, New York, NY.
- Maras, M.-H., 2024. *Real Criminology*. Oxford University Press, New York, NY forthcoming.
- Maras, M.-H., Arsovka, J., 2023. Maras and Arsovka, Understanding the Intersection Between Technology and Kidnapping: A Typology of Virtual Kidnapping. International Criminology 3, 162–176. <https://doi.org/10.1007/s43576-023-0091-4>.

- McGuire, M., Dowling, S., 2013. Cyber crime: A review of the evidence. Summary of key findings and implications. *Home Off. Res. Rep.* 75, 1–35.
- Michael Bullock v. Jessica Doe and John Does i-xx and - 119,873.29 U.S. dollar coin and 119,873 Tether Virtual Currency and - Bam management US holdings Inc.; Bam trading services, inc. d/b/a Binance.us; Payward ventures, inc. d/b/a Kraken; circle internet financial, LLC d/b/a Circle; and Tether operations limited d/b/a a Tether, Case 3:23-cv-03042, Verified Complaint (United States District Court, Northern District of Iowa Central Division, October 19, 2023).
- Michaelson, R., 2023. Turkish presidential candidate quits race after release of alleged sex tape. *Guardian* (11 May 2023). <https://www.theguardian.com/world/2023/may/11/muharrem-ince-turkish-presidential-candidate-withdraws-alleged-sex-tape> (Accessed 13 February 2024).
- Middle East North Africa Financial Network, 2022. Crypto Scams on Tinder Rise: Cyber-Forensics.Net Explains How Cryptorom Scams Work on Tinder, And How to Avoid Them? (NexisUni database). MENAFN, May 2, 2022. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:6698-G2J1-JBR8-B2PJ-00000-00&context=1516831> (Accessed 13 February 2024).
- Middle East North Africa Financial Network, 2023. Minnesota Crypto Scam Costs Couple Over \$9 Million (NexisUni database). MENAFN - Press Releases (English), 3 August 2023. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:68VS-V9F1-DY6B-21XP-00000-00&context=1516831> (Accessed 13 February 2024).
- Newman, L.H., 2023. Hacker Lexicon: What Is a Pig Butchering Scam? *Wired*, January 2, 2023. <https://www.wired.com/story/what-is-pig-butchering-scam/> (accessed 5 November 2023).
- OKX.com, *Elaine Kim Chen: Yu, Does 1-15, and Does:16-20, case 23-0180*, Case 23-0180, Summary Order to Cease and Desist (Investor Protection Director for the State of Delaware, September 15, 2023).
- Owczarzak, B., 2023. Man loses \$35K in 'pig butchering' scam (NexisUni database). CNN Wire, 6 July 2023. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:68MP-0BX1-JBS-S0S7-00000-00&context=1516831> (Accessed 13 February 2024).
- Pawaon, R., 2023. CryptoRom Scammers Add AI Chat Tool, Like ChatGPT, and Fake Hacks on Crypto Accounts Their Toolset. Sophos Finds (NexisUni database). Mid-East. Info, 7 August 2024. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:68WJ-66M1-JDJN-64W3-00000-00&context=1516831> (Accessed 13 February 2024).
- Pepper, T., 2023. FinCEN Issues Alert for Financial Institutions on Red Flags for 'Pig Butchering' Schemes (NexisUni database). *Newstex Blogs JD Supra*, 13 September 2023. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:695F-04J1-JCMN-Y1X3-00000-00&context=1516831> (Accessed 13 February 2024).
- Platte-Valley News Channel Nebraska, 2023. Coinrule-Web3.com Emerges as Preferred Financial Investment Platform for American Customers with Exceptional Risk Control and Thoughtful Service. <https://plattevalley.newschannelnebraska.com/story/49417698/coinrule-web3com-emerges-as-preferred-financial-investment-platform-for-american-customers-with-exceptional-risk-control-and-thoughtful-service> (Accessed 5 November 2023).
- Podkul, C., 2022. How to avoid China's 'pig butchering' cyberscams. 2023. (NexisUni database) MENAFN, September 26, 2022. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:66R4-7WF1-DY6B-22PS-00000-00&context=1516831> (Accessed 13 February 2024).
- Roose, K., 2022. Crypto Scammers' New Target: Dating Apps the Shift (NexisUni database) New York Times, 21 February 2022. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:64V1-XBC1-JBG3-61WK-00000-00&context=1516831> (Accessed 13 February 2024).
- Sandhu-Longoria, A.K., 2023. Looking for love? Watch out for romance scams that break your heart (NexisUni database), USA Today, 17 February 2023. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:67K2-1S51-DXGX-60P0-00000-00&context=1516831> (Accessed 13 February 2024).
- Sarker, G., Shukla, S.K., 2023. Behavioral analysis of cybercrime: Paving the way for effective policing strategies. *J. Econ. Criminol.*, 100034. <https://doi.org/10.1016/j.jecon.2023.100034>
- Scamwatch, 2021. Romance baiting scams on the rise. National Anti-Scam Centre, Australia <https://www.scamwatch.gov.au/about-us> (Accessed 5 November 2023).
- Schoeff, M., Jr., 2023. Investors continue to get roasted in pig-butchering schemes (NexisUni database). *InvestmentNews* (10 July 2023). <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:68NK-DWX1-JC7X-W3T7-00000-00&context=1516831> (Accessed 13 February 2024).
- Skores, A., 2023. Here's how dating app Match Group is fighting romance scammers. *Tampa Bay Times*, January 13, 2023. <https://www.tampabay.com/news/nation-world/2023/01/13/match-dating-scams-tinder-hinge-plenty-of-fish-meetic-ourtime/> (Accessed 5 November 2023).
- Sophos, 2023a. Sophos Reports: Scammers Employ Bogus Cryptocurrency Trading Pools in Sha Zhu Pan Scheme, Siphoning Over \$1 Million (NexisUni database). CXOToday.com, 6 October 2023. <https://www.sophos.com/en-us/press/press-releases/2023/09/sha-zhu-pan-scammers-use-fake-cryptocurrency-trading-pools-steal-more> (Accessed 13 February 2024).
- Sophos, 2023b. Sophos Investigates Two Active Cyberfraud Operations, Indicating Scammers are Expanding Their Crypto-Romance Cons, <https://www.sophos.com/en-us/press/press-releases/2023/02/cyberfraud-operations-indicate-scammers-are-expanding-their-crypto-romance-cons> (Accessed 15 February 2023).
- State News Service, 2022a. Cryptocurrency Broker Unisom FX Limited Appears to be Engaged on Fraud Against California Consumers (NexisUni database). December 27, 2022. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:6766-B6S1-JCBF-S37K-00000-00&context=1516831> (Accessed February 13, 2024).
- State of Indiana vs XU XIONGJU, LI KUN, HU JIAJIAN, HAN ZHAOQING, and DIN TAY TRAN, Case No. 29D07-2303-MI-002357, Complaint for Damages, Forfeiture of Property, Seizure of Assets and for Injunctive Relief. Jurisdiction (Hamilton County Superior Court 7, June 27, 2023).
- State of Michigan Attorney General, Consumer Protection Team, n.d. Cryptocurrency Scam - Pig Butchering. <https://www.michigan.gov/consumerprotection/protect-yourself/consumer-alerts/scams/cryptocurrency-scam-pig-butchering> (Accessed 28 December 2023).
- States News Service, 2022b. Cryptocurrency broker ZC exchange appears to be engaged in fraud against California consumers (NexisUni database). 27 December 2022. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:6766-B6S1-JCBF-S37R-00000-00&context=1516831> (Accessed February 13, 2024).
- U.S. Attorney's Office, Central District of California, 2023. Justice Dept. Seizes Over \$112M in Funds Linked to Cryptocurrency Investment Schemes, With Over Half Seized in Los Angeles Case. <https://www.justice.gov/usao-cdca/pr/justice-dept-seizes-over-112m-funds-linked-cryptocurrency-investment-schemes-over-half> (Accessed 3 April 2023).
- U.S. Attorney's Office, Eastern District of Virginia, 2022. Court Authorizes the Seizure of Domains Used in Furtherance of a Cryptocurrency "Pig Butchering" Scheme. <https://www.justice.gov/usao-edva/pr/court-authorizes-seizure-domains-used-furtherance-cryptocurrency-pig-butchering-scheme>. (Accessed 5 November 2023).
- U.S. Attorney's Office, District of New Jersey, 2022. Middlesex County Man Charged with Laundering \$2.1 Million Obtained from Internet-Related Frauds (NexisUni database). October 11, 2022. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:66MC-H111-DYVR-P3GG-00000-00&context=1516831> (Accessed 13 February 2024).
- U.S. Department of Financial Protection and Innovation, 2022a. Cryptocurrency broker RB Hood appears to be engaged in fraud against California consumers. <https://dfpi.ca.gov/2022/12/28/cryptocurrency-broker-rb-hood-appears-to-be-engaged-in-fraud-against-california-consumers/#:~:text=Cryptocurrency%20broker%20RB%20Hood%20appears%20to%20be%20engaged%20in%20fraud%20against%20California%20consumers,-Dec%202028%2C2022&text=The%20California%20Department%20of%20Financial,resident%20regarding%20a%20crypto%20investment> (Accessed 13 February 2024).
- U.S. Department of Financial Protection and Innovation, 2022b. Cryptocurrency Broker ZC Exchange Appears to be Engaged in Fraud Against California Consumers. <https://dfpi.ca.gov/2022/12/27/cryptocurrency-broker-zc-exchange-appears-to-be-engaged-in-fraud-against-california-consumers/#:~:text=Cryptocurrency%20Broker%20ZC%20Exchange%20appears%20to%20be%20engaged%20in%20fraud%20against%20California%20consumers,-Dec%202027%2C2022&text=The%20California%20Department%20of%20Financial,resident%20regarding%20a%20crypto%20investment> (Accessed 13 February 2024).
- U.S. Department of Financial Protection and Innovation, 2022c. Cryptocurrency Broker Unisom FX Limited Appears to be Engaged on Fraud Against California Consumer. <https://dfpi.ca.gov/2022/12/27/cryptocurrency-broker-unisom-fx-limited-appears-to-be-engaged-in-fraud-against-california-consumers/> (Accessed 13 February 2024).
- U.S. Department of Justice, 2023. On Valentine's Day, Attorney General Bonta Warns Californians Against Romance Scams. <https://oag.ca.gov/news/press-releases/valentine%2080%99s-day-attorney-general-bonta-warns-californians-against-romance-scams> (Accessed 28 December 2023).
- U.S. Fed News, 2023. Investor Protection Unit Grills "Pig Butchering" Scammers. (NexisUni database). 28 September 2022. <https://advance-lexis-com.ez.lib.jjay.cuny.edu/api/document?collection=news&id=urn:contentItem:66GY-B2P1-F12F-F18D-00000-00&context=1516831> (Accessed 13 February 2024).
- United Nations Human Rights Office of the High Commissioner, 2023. Online Scam Operations and Trafficking into Forced Criminality in Southeast Asia: Recommendations for a Human Rights Response. <https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf> (Accessed 5 November 2023).
- United States of America v. \$811,549.41 in Bank Funds in Citibank Account '1187, \$729,981.00 in Bank Funds in Cathay Bank Account '7026, \$228,331.19 in Bank Funds in Citizens Bank Account '0334, \$159,091.41 in Bank Funds in West Bank Account '8584, and \$100,000.00 in Bank Funds in East West Bank Account '5043, Case: 2:23-cv-08774-MCS-AJR, Verified Complaint for Forfeiture (U.S. District Court for the Central District of California, October 18, 2023).
- United States of America v. 5,012,294.90 in TetherUS ("USDT"), 75,589,553.41 in Gala ("GALA"), 226.81 in BNB ("BNB"), 1,264.16 in Bitcoin ("BTC"), 1,495.72 in Lentry ("LIT"), 48,969 in Fantom ("FTM"), 47.17 in Ethereum ("ETH"), 501.41 in USD ("USD"). Case 2:23-cv-01988-JJT, Verified Complaint for Forfeiture in Rem (U.S. District of Arizona, September 20, 2023).
- United States of America v. 56,382,970 Tether Seized from Binance Account Ending 1678; and 0.03001485 Ether Seized from Binance Account Ending 1678, Case 1:23-cv-04861-at, Verified Complaint for Forfeiture (United States District Court or the Northern District of Georgia Atlanta Division, October 23, 2023).
- United States of America v. Approximately 1, 360,000.748 Tether and \$3,859,703.65 in U.S. Currency, Case 3:23-cv-04400, Verified Complaint for Civil Forfeiture in REM (U.S. District Court Northern District of California San Francisco Division, August 25, 2023).
- United States of America v. Approximately 503, 349.86 Tether, 1,379,999 Cardano, and 163,118 Binance USD, Case 3:22-cv-05199-tlt, Verified Complaint for Civil Forfeiture in REM (United States District Court Northern District of California San Francisco division, September 7, 2022).
- United States of America v. Jin Hua Zhang, Gregory Armand, Chen Chen, Yanbin Chen, Changgui Huang, Xin Jin, Jiahui Miao, LingMing Zeng, Jin Fu Zhang, and Hua Zhou, Criminal Indictment, Case No. 1:22-cr-00458-LDH (U.S. Eastern District of New York, October 14, 2022).

- United States of America v. Hailong Zhu, Case 1:23-mj-00063-IDD, Affidavit in Support of a Criminal Complaint and Arrest Warrant: Case Images (U.S. District Court for the Eastern District of Virginia, March 10, 2023a).
- United States of America v. Hailong Zhu, Case 1:23-mj-00063-IDD, Affidavit in Support of a Criminal Complaint and Arrest Warrant (U.S. District Court for the Eastern District of Virginia, March 10, 2023b).
- United States of America v. Hailong Zhu, Case 1:23-sw-372, Indictment (U.S. District Court for the Eastern District of Virginia, March 10, 2023c).
- United States of America v. Hailong Zhu, Case 1:23-sw-00372-JFA, Affidavit in Support of Seizure Warrant (U.S. District Court for the Eastern District of Virginia, March 10, 2023d).
- United States of America, v. 1. 12,324.84 USDT Seized from Binance.com User ID # 2974 in the name of Duean Phikunkaew; 2. Cryptocurrency Seized from Binance.com User ID # 0476 in the name of Varat Vitthayanuwat; 3. Cryptocurrency Seized from Binance.com User ID # 5033 in the name of Wang Xuewen; 4. 6,972.2 USDT Seized from Binance.com User ID # 3307 in the name of Jiang Changsen, Case 1:23-cv-02549, Verified Complaint for Forfeiture in REM (U.S. District Court for the District of Colorado, September 29, 2023).
- United States of America, v. Zeshawin Stanley, Case 2:21-cr-00099-mcs document 67, (U. S. District Court for the Central District of California, March 17, 2023).
- United States of America, v. 86,766.00 USDT Seized from OKY Account UUID ending 5504 and id number '097799 with affiliated deposit address ending 94d8, Case 1:23-cv-0116, Verified Complaint for Forfeiture in REM (United States District Court Western District of Michigan Southern Division, November 23, 2023).
- UNODC, 2013. Draft Compt. Study Cyber (https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG_4_2013/CYBERCRIME_STUDY_210213.pdf (Accessed 13 February 2024)).
- UNODC, 2019. Cybercrime module 2 introduction and learning outcomes. Teach. Modul. Ser. Cyber (<https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-2/introduction-and-learning-outcomes.html> (Accessed 16 March 2023)).
- UNODC, 2022. Digest of Cyber Organized Crime, second ed. United Nations, Vienna.
- Wall, D., 2007. Cybercrime: The Transformation of Crime in the Information Age. Polity.
- Wall, David S., 2015. Dis-organised crime: towards a distributed model of the organisation of cybercrime. 2015. Eur. Rev. Organ. Crime. 2 (2), 71–90. <https://doi.org/10.2139/ssrn.2677113>
- Wang, F., Zhou, X., 2023. Persuasive schemes for financial exploitation in online romance scam: an anatomy on Sha Zhu Pan in China. Vict. Offenders 18 (5), 915–942. <https://doi.org/10.1080/15564886.2022.2051109>
- Wang B. Denver man loses \$1.6 million in new “Pig Butchering” cryptocurrency scam. Denver7 ABC, December 20 2021 2021. <https://www.denver7.com/news/contact-denver7/denver-man-loses-1-6-million-in-new-pig-butchering-cryptocurrency-scam>.
- Whittaker, J.M., Lazarus, S., Corcoran, T., 2024. Are fraud victims nothing more than animals? Critiquing the propagation of “pig butchering” (Sha Zhu Pan, 杀猪盘). J. Econ. Criminol. 3, 100052. <https://doi.org/10.1016/j.jeconc.2024.100052>
- Whitty, M., 2013. The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. Br. J. Criminol. 53 (4), 665–884. <https://doi.org/10.1093/bjc/azt009>
- Whitty, M.T., Buchanan, T., 2016. The online dating romance scam: the psychological impact on victims - both financial and non-financial. Criminol. Crim. Justice 16 (2), 176–194. <https://doi.org/10.1177/1748895815603773>
- Wiederhold, B.K., 2020. Internet dating: should you try it? Cyber, Behav., Soc. Netw. 23 (4), 195–196. <https://doi.org/10.1089/cyber.2020.29178.bkw>
- Zimwara, T., 2023. Namibian Police Arrest 20 Ringleaders of Local Pig Butchering Crypto Scam. Crypto Break. N. (October 18, 2023. <https://news.bitcoin.com/report-namibian-police-arrest-20-ringleaders-of-local-pig-butchering-crypto-scam/> (Accessed 13 February 2024)).
- Zuo, M., 2021. Online ‘pig butchering’ love scams have gone global after getting their start in China. South China Morning Post. <https://www.scmp.com/news/people-culture/social-welfare/article/3150688/online-pig-butchering-love-scams-have-gone> (Accessed 5 November 2023).

'Pig butchering' crypto scam: Americans taking their lives after losing savings to international criminal gangs

cnn.com/2024/06/17/asia/pig-butchering-scam-southeast-asia-dst-intl-hnk/index.html

By Teele Rebane and Ivan Watson, CNN

June 17, 2024

Editor's note: If you or someone you know is struggling with suicidal thoughts or mental health matters, please call the 988 Suicide & Crisis Lifeline in the US by dialing 988 to connect with a trained counselor, or visit the [988 Lifeline website](#). For support outside of the US, a worldwide directory of resources and international hotlines is provided by the [International Association for Suicide Prevention](#). You can also turn to [Befrienders Worldwide](#).

CNN —

Sitting at the kitchen table, Matt struggles to recount the events of the past few months. "As soon as I found out that it was a suicide, I was 100% sure that it was the scam," he says.

"Our father was, from the day I was born until six months ago, always a positive, happy person. This was literally the only thing in his life that had happened, to where it changed him, and it just crushed him."

On a horse farm in northern Virginia, surrounded by sprawling fields and stables, the family gathers at their younger sister Adrienne's house - something they've done a lot in the three months since their father took his own life after falling victim to a so-called "pig butchering" scam.



Loving father Dennis Jones, 82, withdrew from his family and after he befriended a woman going by the name Jessie on Facebook.

CNN

The scams – mostly run out of Southeast Asia - are given that name because they involve “fattening up” victims before taking everything they have. The con artists behind them take on false online identities and spend months financially grooming their victims to get them to invest on fraudulent cryptocurrency websites.

Dennis Jones, an avid runner and photographer, was adored by his children and grandchildren. Described as “a bit of an activist” by his family, the 82-year-old spent much of his retirement working with refugees and debating politics online. But in the last few months of his life he withdrew from his family and, having been divorced for years, befriended a woman going by the name Jessie on Facebook.

The two had been talking online for months and built a close relationship. Eventually, Jessie convinced Dennis to invest in crypto.

Dennis complied. Without ever meeting Jessie in person, he spent everything he had, and when he had nothing left, she demanded more. Until one day the money disappeared, leaving him in ruin.

In early March, Dennis’ children scheduled a meeting to help their father get back on his feet after the scam. The plan was for him to move in with Adrienne and her family. “We wanted him to know that he was going to be taken care of,” Matt said.



Matt and Adrienne lost their father Dennis to suicide in March after he fell victim to a cryptocurrency investment scam.

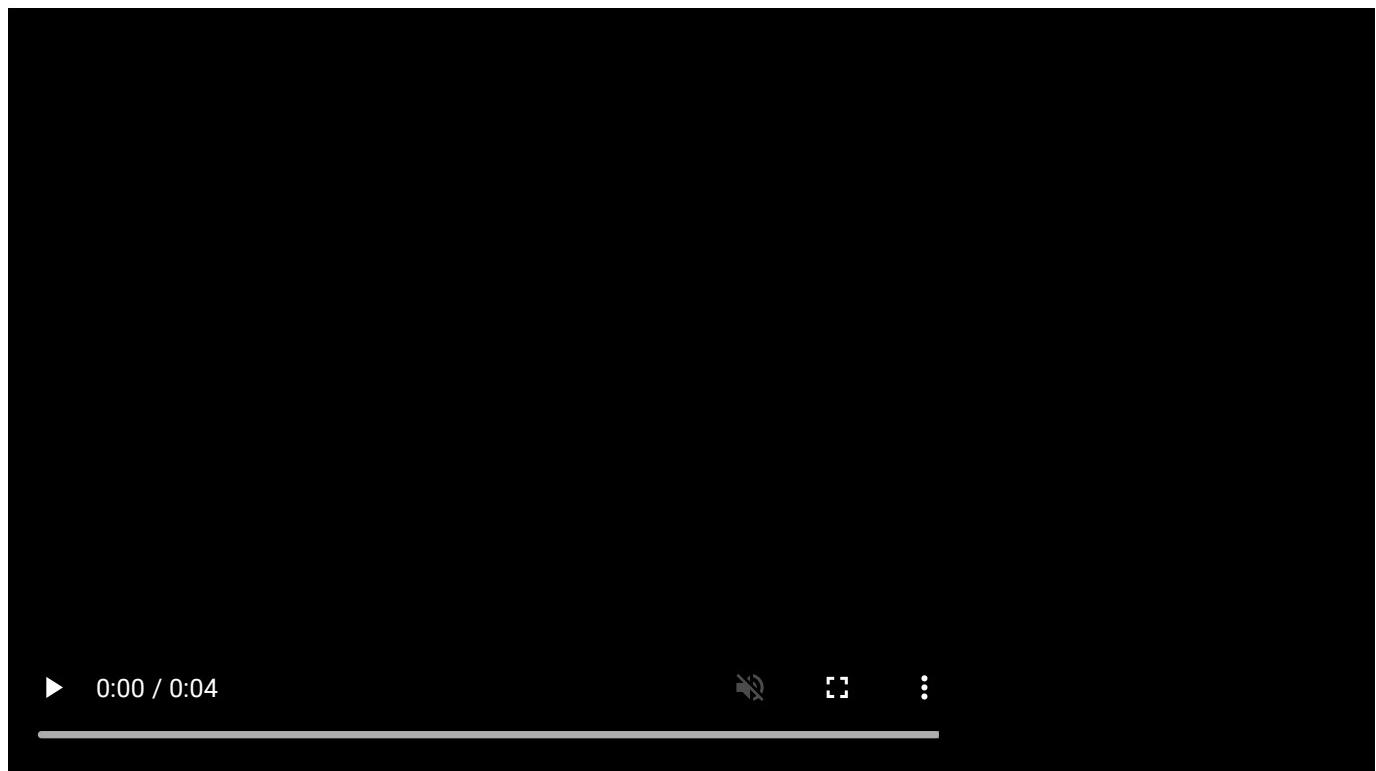
CNN/Chris Turner and Amanda Swinhart

But the morning of the meeting none of them could reach Dennis. Matt drove to Dennis's apartment but he wasn't home, and all calls went straight to voicemail. They figured he must be out on one of his long runs. An hour later, police knocked on Matt's door to inform him that Dennis had taken his own life.

Dennis was one of countless victims of a massive global criminal operation predominantly run by Chinese gangs who have built a multibillion-dollar scam industry in Southeast Asia. There, they've assembled an army of scammers, many held against their will in guarded compounds and forced to con people all around the world out of their life savings.

It's theft at a scale so large that investigators are now calling it a mass transfer of wealth from middle-class Americans to criminal gangs. Last year, the FBI estimates, pig butchering scams stole nearly \$4 billion from tens of thousands of American victims, a 53% increase from the year before.

While the crime takes place online, its real-world consequences are devastating. Law enforcement sources predict that losses will continue to grow in the next year, and as the criminals remain out of reach, money and lives will continue to be lost.



Dennis grew desperate as he struggled with the financial and emotional impact of the scam.

CNN

'Victims victimizing victims'

Santa Clara county prosecutor Erin West has dedicated the last few years to fighting pig butchering scams. "I've been a prosecutor for over 25 years, I've done all kinds of different types of crime. I spent nine years in sexual assault. And I've never seen the absolute decimation of people that I've seen as a result of pig butchering," she says.

Being in the heart of the tech industry in California's Bay Area, Erin and her team were some of the first to begin investigating pig butchering scams. "We've got victims victimizing victims and the only winners are Chinese gangsters," she says.

Shawn Bradstreet, US Secret Service special agent in charge of the San Francisco field office, told CNN that some of the money stolen from American victims is spent on expanding the scam operations and the massive compounds that house them and other illicit activities.



Santa Clara county prosecutor Erin West is part of a small group of US law enforcement agents working to find ways to tackle pig butchering scams.

Jim Castel/CNN

West and Bradstreet are part of a small group of US law enforcement agencies working to find ways to tackle a crime that largely takes place online and overseas.

Social media is flooded with scammers hunting for victims, on WhatsApp, Facebook, LinkedIn and, increasingly, dating apps such as Bumble and Tinder.

"The unfortunate reality is that scammers may pull on the heartstrings on those looking for love or connection - on dating apps and on all online platforms," a spokesman for Match group, which owns Tinder, said in a statement.

Match, Bumble, Facebook and Whatsapp parent company Meta told CNN they are working to prevent scammers from using their platforms, by flagging suspicious language and educating their users. In a statement to CNN a Bumble spokesperson said they have introduced AI to help identify spam, scam and fake profiles "aiming to take action before such profiles have the opportunity to interact with members." CNN has reached out to LinkedIn for comment.

In May, a group of tech companies including cryptocurrency exchange platform Coinbase, Meta, Match group and the anti-scam charity organization GASO announced the “Tech Against Scams Coalition,” acknowledging that scams “are a pervasive issue across the entire tech landscape.”

'PIG BUTCHERING' A sophisticated criminal network is using modern-day slaves to con Americans out of their life savings

But West says that's not enough. She recently set up a task force called Operation Shamrock to bring together law enforcement, social media, crypto exchanges and traditional banks to tackle crypto scams.



A 2023 CNN investigation revealed that many of the scammers are themselves victims of human trafficking. Lured to Southeast Asia with promises of white-collar jobs, they are instead trafficked into Myanmar, Cambodia, Laos and other destinations. Since a 2021 military coup, Myanmar has become Asia's scam capital where criminals can operate freely under the cover of a bloody civil war.

Today, city-sized compounds loom over the Myanmar side of the border with Thailand, with nothing but a dried-out river separating the two countries. Inside are what can only be described as scam factories — offices full of hundreds of slaves, working 16-hour days to befriend victims and convince them to invest in cryptocurrency on fake platforms that mimic legitimate crypto exchanges.

Those kept inside tell stories of torture and abuse, of scammers who don't bring in enough money being beaten with electrical sticks and forced to do hundreds of squats as punishment.



In November 2023, CNN visited the Thai-Myanmar border region where dozens of city-sized compounds loom over the Myanmar side.

CNN/Tom Booth

Rakesh, an Indian national, was trafficked to a compound called Gate 25 in Myanmar after applying for an IT job in Thailand in late 2022. There he signed a scamming contract under threat of execution, and was trained to scam.

“

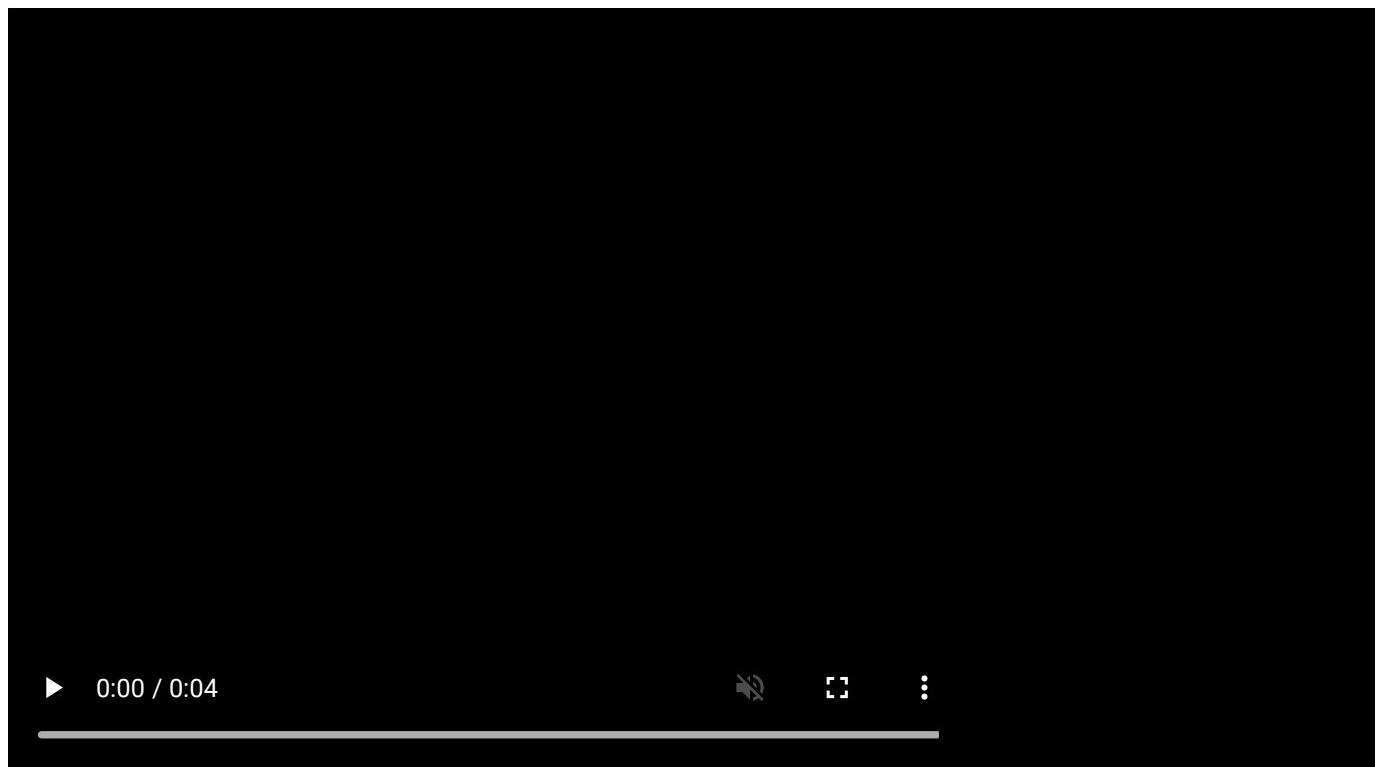
They (were) treating us like slaves.

Rakesh, trafficking victim

For 11 months he posed as “Klara Semonov,” a Russian investor based in Salt Lake City. To avoid gruesome punishments inflicted by his captors, he said he sent romantic messages to victims like Dennis to convince them to invest their money. “Seventy to 80% fall for fake love,” he said.

Rakesh was eventually released in 2023 when his contract ended. He believes he was let go because he simply wasn’t good enough at scamming. “They (were) treating us like slaves,” he told CNN days after his release in 2023.

Conveniently located on the border, the compounds use telecoms services from the Thai side. In November 2023 Thai Justice Minister Tawee Sodsong said they were working to cut off the compounds.



Rakesh spent 11 months forced to work against his will at a scam compound in Myanmar, posing to potential victims as a US-based Russian investor.

CNN/Tom Booth

Pachara Naripthaphan of the Thai National Broadcasting Transmissions Commission has since told CNN that in May they instructed all telecom operators to shut off wireless services in proximity to any areas bordering Myanmar, Laos or Cambodia. Despite that, their data shows that illicit activity has continued at a baseline level as criminals adjust to using other means of connecting to the internet such as Starlink.

Even here on the border, where the physical distance is reduced to nothing but a narrow river, the criminals remain out of the reach of law enforcement, either locally or internationally.

“Many of these perpetrators are beyond my reach. And in order to establish deterrence, we need to prosecute some individuals who are running these operations in Southeast Asia,” Santa Clara district attorney Jeff Rosen says.

According to FBI data, out of nearly \$5 billion dollars lost to cryptocurrency fraud in 2023, \$3.96 billion was stolen in pig butchering scams. While Rosen’s office and the Secret Service have had some success in retrieving millions of dollars in stolen funds, no American law enforcement agency has been able to arrest a single suspected scammer.

‘Hard to believe’

Carina, who asked CNN to only use her first name, met “Evan” on Bumble in May 2023. His photos showed a blond man with piercing blue eyes. He claimed to be Dutch and showed off his wealth — expensive cars and Rolexes, though none of that appealed to Carina, a chemistry PhD and triathlete.

Their relationship moved fast. Right away he suggested they move their conversation to WhatsApp and delete the Bumble app to focus on getting to know each other. A few days later he started calling her “honey.”

“We’re doing that already?” Carina asked, in a text conversation seen by CNN.



Carina met her scammer "Evan Van" on the dating app Bumble.

Jim Castel/CNN

Evan claimed he had made his money running a company with his uncle and investing in crypto. He told her she could pay off her student loans in a matter of months by investing. Carina was hesitant at first but eventually agreed to put in \$1,000.

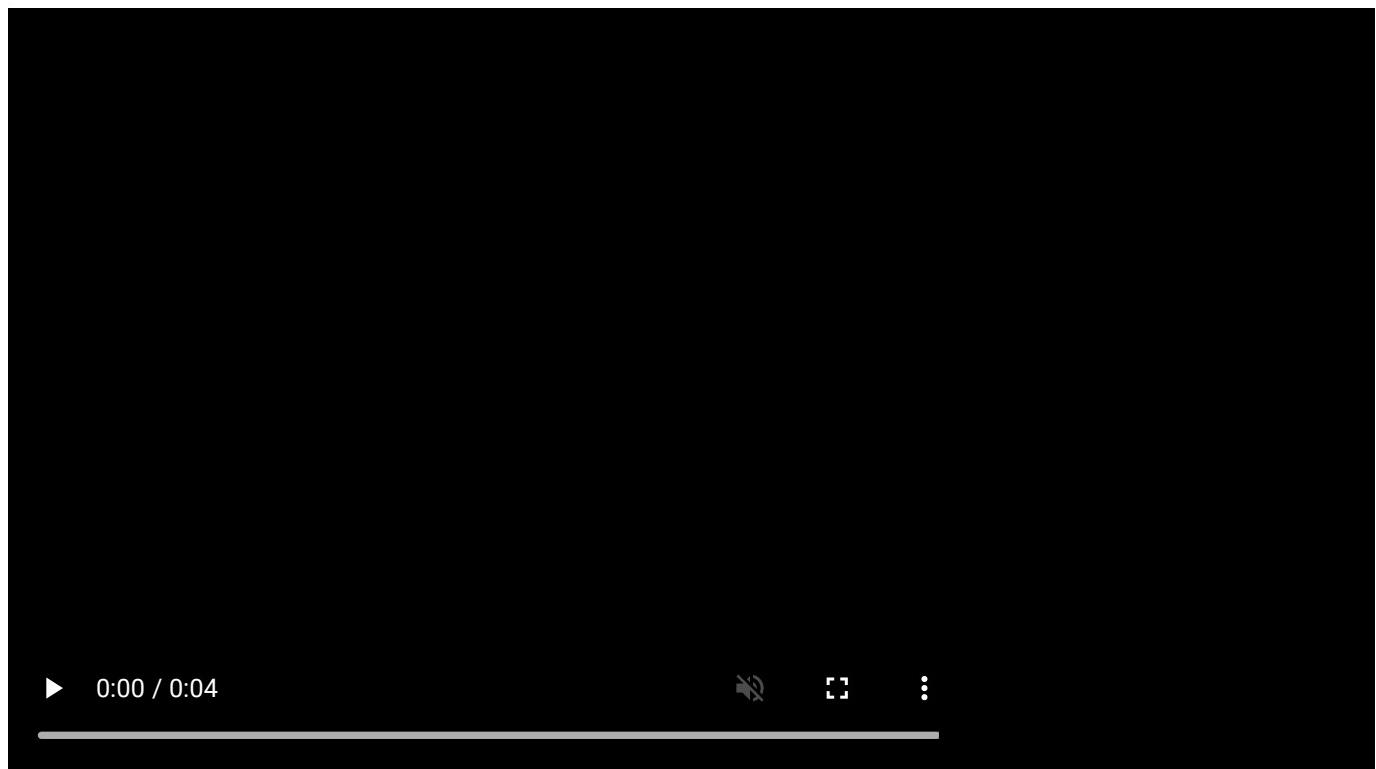
He told her not to use the official app of the Kraken crypto platform, and instead sent her a link to a parallel website which they used to trade in the coming months.

As their investments grew, so did their relationship. The two made plans for the future, romantic weekend getaways and family introductions, though they were yet to meet in person. "I've never met anyone like you before. Hard to believe I'm falling for a man I have never seen or spoken to," Carina told him just a few weeks in.

The first red flag emerged when Evan pressured Carina to enter an "event" where she would have to invest \$150,000 by the end of July to make extra profit. If she failed to reach the target, her account and money would be frozen.

Scared to lose the money she had already put in, Carina panicked. She took out a high-interest loan and borrowed money from friends and family to meet the deadline.

Despite all his purported wealth, Evan refused to help her, instead lying and telling her he was struggling to meet his target of \$500,000 and needed her help, she said. At one point, Carina found herself consoling her scammer, telling him the money didn't matter as long as they loved each other.



Carina spent hours every day chatting and falling in love with her scammer "Evan."

CNN/Jim Castel

'Major psychological stunt'

After Dennis took his life, his adult children were left piecing together what happened by going through his Facebook messages. There, they learned for the first time what Dennis had been dealing with.

"I have been having dark thoughts about my life and it being over. Certainly it looks like my financial life is done," Dennis messaged his scammer in the months before his death. "And the ultimate pain here is that I have betrayed family trust. This is unbearable," he writes in screenshots of their conversation seen by CNN.

"What's most heartbreakingly is reading through these messages. He was talking about having signs of a nervous breakdown. And so these were all shared with the profile," Adrienne says.

"Instead of sharing with us," Matt adds.

"What's amazing here is that these scammers overseas have figured out a way that they can get victims to trust them over their own families," West says. "It's a major psychological stunt that they're pulling on the rest of the world."

“

It was all fake. It was a fake profile. It was a fake story.

Carina, scam victim

Carina didn't tell her family about what had happened and the stress she was under until the very final moment. After hitting their event targets, Carina tried to withdraw some of her money, but was unable to do so, having violated platform rules by investing in the same account as Evan. After months of hiding it, Carina told her family, who suggested she speak to Kraken directly.

How to get help

Help is available if you or someone you know is struggling with suicidal thoughts or mental health matters.

In the US: Call or text 988, the [Suicide & Crisis Lifeline](#).

Globally: The [International Association for Suicide Prevention](#) and [Befrienders Worldwide](#) have contact information for crisis centers around the world.

The next morning she called Kraken customer services, who informed her there was no account under her name.

"I realized I had been scammed at that point. And I broke down," Carina says. "It was all fake. It was a fake profile. It was a fake story. The amount of time that he spent grooming and getting to know me was incessant."

Reading through their conversations a year later, Carina barely recognizes herself. "It's actually heartbreaking for me to see the state that I was in," she says.

The emotional and financial entanglement had taken a toll on her, and she was left reeling from a breakup and bankruptcy at the same time.

In the aftermath, Carina had to move back in with her mother. It will take her at least a decade to repay her debts.

'Playing on emotions'

Their grief still raw, Adrienne and Matt are only now starting to understand what happened to their father.

"He wasn't up against one person. It's a multibillion-dollar criminal organization with a playbook that's playing on the emotions ... It was almost like he was brainwashed to some extent," Dennis' daughter Adrienne says.

As the criminals' tactics continue to evolve and law enforcement struggles to find a way to stop them, there will be more victims in 2024, and more people like Matt and Adrienne, who suffer a loss far greater than money.

"He died embarrassed, ashamed, financially devastated, heartbroken. And if sharing our story helps somebody else or another family, then it's worth it," Adrienne says.

If you think you are a victim of a cyber scam the FBI recommends you report to the Internet Crime Complaint Center (IC3) at <https://www.ic3.gov/Home/ComplaintChoice>

This story has been updated.

CNN's Kocha Olarn in Bangkok contributed to this report